1984

Reliability analysis for the emergency power system of a pressurized water reactor facility during a loss of offsite power transient

See-Meng Wong
Iowa State University

INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.

2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of "sectioning" the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again–beginning below the first row and continuing on until complete.

4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.

University
Microfilms
International
300 N. Zeeb Road
Ann Arbor, MI 48106

Wong, See-Meng

RELIABILITY ANALYSIS FOR THE EMERGENCY POWER SYSTEM OF A PRESSURIZED WATER REACTOR FACILITY DURING A LOSS OF OFFSITE POWER TRANSIENT

Iowa State University PH.D. 1984

Reliability analysis for the emergency power system of a pressurized water reactor facility during a loss of offsite power transient

by

See-Meng Wong

A Dissertation Submitted to the

Graduate Faculty in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Departments: Nuclear Engineering
Electrical Engineering and Computer Engineering

Co-Majors: Nuclear Engineering
Electrical Engineering and Computer Engineering
(Electric Power)

Approved:

Signature was redacted for privacy.

In Charge of Major Work

Signature was redacted for privacy.

For the Major Departments

Signature was redacted for privacy.

For the Graduate College

Iowa State University
Ames, Iowa

1984

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

The emergency power system (EPS) for a typical pressurized water reactor (PWR) power generating facility is designed to supply power to the reactor protection system (RPS) for safe shutdown. It also provides power for the engineered safety features (ESF) system that is intended to mitigate the consequences of transients (anticipated or unanticipated) or accidents. The EPS consists of: 1) offsite ac power (the preferred source), 2) onsite ac power (the standby source), 3) dc power, and 4) auxiliary equipment for the distribution of power to the ESF loads.

A hypothetical sequence of events associated with the EPS had been identified in the Reactor Safety Study (RSS) to be a major contributor of risk for a core meltdown accident [1]. This sequence of events involves a loss of offsite power (LOSP) during a loss-of-coolant accident (LOCA), compounded by failure of the emergency onsite power supply and auxiliary feedwater delivery. Whether this postulated scenario (referred to as the TMLB' sequence in the RSS) may or may not be a major risk contributor during routine operating conditions, it represents one of the most severe challenges for any nuclear power plant.

The onsite power system (i.e., the emergency diesel generators) should assume the full ESF loads within thirty (30) seconds after a LOSP coincident with a large LOCA. This capability is significant in retarding the progression of this sequence of events and in mitigating the effects of a probable core meltdown. If there is a total loss of electrical power supply to the ESF system for about an hour after a LOCA, core cooling

gradually declines. Hence, a systematic reliability analysis of the EPS is important in the optimal design of the electrical power distribution system in a commercial nuclear power plant. In particular, the availability of redundant diesel generators should be investigated for its impact on avoiding or reducing the effects of the postulated core meltdown sequence.

This dissertaion examines the reliability of the EPS and its impact on overall plant safety using probabilistic risk assessment (PRA) techniques. The analysis is performed using the reliability block diagram (RBD) model and fault tree logic in PRA methodology. This provides a comprehensive approach to the quantitative and qualitative assessment of system reliability. The RBD model represents the active elements of a system in "supercomponent trains" which permit the identification of system-success pathways for reliability prediction. The fault tree process is a powerful tool for analyzing the possible mechanisms for failure of system functions including human interactions and initial system parameters in addition to multiple component failures. The RBD adds clarity to the quantification of the fault tree in estimating overall system availability.

The course of a postulated accident is analyzed by event tree methodology to complement the PRA effort. The event tree identifies the possible outcomes of a given initiating event. It provides a useful structure for probabilistic analysis and quantifying the probability of transient events [2]. To analyze the influence of human control over the outcomes of an event initiator, a functional event tree such as the "operator action" event tree (OAET) is used to address the unique role of the individual in mitigating the consequences of a significant event.

Finally, the unavailability of the EPS represents a common cause failure of great importance in the operational design of the electrical power distribution system of a nuclear power plant. Enhanced system reliability contributes to improvement in overall plant availability. The successful automatic responses to a LOSP initiator and the relevant operator actions to retard the progression of undesirable plant conditions result in overall increased safety during routine operations.

II. RESEARCH OBJECTIVES

The Reactor Safety Study (RSS) identified the anticipated transient involving loss of offsite power (LOSP) as a potential major contributor of risk for the pressurized water reactor (PWR) power plant that was under investigation [1]. It was estimated that LOSP occurs about ten (10) times per year per reactor [1, 3]. In addition, the evaluation of risks from this particular accident scenario, using the CORRAL computer code, indicates that this sequence of events is a significant contributor to PWR containment releases [3]. The CORRAL code estimates the magnitude of radioactivity released to the atmosphere [3].

The total loss of power on the offsite electrical grid can be caused by a main generator outage due to an abnormal plant transient, or by external events such a lightning, tornadoes, storms and fire. The automatic responses to the LOSP initiator include trips of: the reactor (scram), the reactor coolant pumps, the main turbine, the main feedwater pumps and the circulating water pumps. Emergency feedwater is delivered to the steam generators by the turbine-driven emergency feedwater pump when low steam generator water level is reached. The standby diesel generators are automatically started to begin their designated loading sequence. The two motor-driven emergency feedwater pumps will have been sequenced to provide additional emergency feedwater flow. Decay heat is removed by steam relief from the steam generators. Primary coolant inventory and pressure are controlled by the charging pumps (or high pressure safety injection flow) and pressurizer heaters.

The RSS analyzed the various individual accident paths having the potential to cause core degradation, but it did not adequately address the safety problem that can arise when faults in one system cause failure of an interrelated or entirely different system. While human error was treated as a unique contributor to system failures, there was insufficient attention to correlated or sequential operator faults. In the PRA effort, the RSS also did not account for design errors [4].

The TMI-2 (Three-Mile Island-2) incident has supported justification of regulatory requirements for supplementary quantitative reliability analysis plus the evaluation of consequences of system failure [5]. The Advisory Committee on Reactor Safeguards (ACRS) considers that better data are necessary to evaluate the validity of quantitative results from the RSS in absolute terms [4]. The probabilistic evaluation of the full accident spectrum provides quantitative risk criteria that can be employed judiciously in the nuclear licensing process. Quantitative risk assessment is an important input into the decision-making process regarding acceptability for other technologies.

Based on these considerations, the principal objectives of this dissertation are to:

1. Evaluate the reliability, using a reliability block diagram model, of the emergency power system to perform its desired mission.
2. Analyze the fault tree constructed for the emergency power system to yield an assessment of overall system availability. The quantitative evaluation of system availability is based on

updated failure rate estimations of multiple components, operator interactions and common mode failures associated with the emergency power system.

3. Identify the response of the principal nuclear reactor plant systems to the anticipated transient using the event tree methodology and address the role of the operator in the mitigation of the transient.

III. LITERATURE REVIEW

The Reactor Safety Study (RSS) was a risk assessment of commercial nuclear power plants that was based on the definition of dependencies between and among safety functions and the engineered safety feature (ESF) systems [1]. It categorized various hypothetical accidents and identified potential weak links for two types of nuclear power plants: the pressurized water reactor (PWR) and the boiling water reactor (BWR) designs. By incorporating human error, test and maintenance, and common cause contributions to system unavailabilities, the study shows the relationship of core melt to containment failure modes that result from system failures.

An important result of the RSS was that, although the probability of a core meltdown accident was very low, the consequences to the public could be significant. The RSS determined that small loss-of-coolant accident (LOCA) sequences and non-LOCA transients are significant contributors to the predicted frequency of core melt for the PWR [3]. The study assumed, very pessimistically, that a core degradation sequence continued inexorably to its conclusion.

A major risk contributor for the PWR investigated in the RSS was a sequence of events involving a loss of offsite power (LOSP) during a LOCA, coincident with failure of emergency onsite power supply and auxiliary feedwater delivery. The sequence of events results in total loss of available ac power to the ESF systems because the LOCA induces a main generator outage. This scenario may be one of the most severe challenges for any nuclear power plant.

It was estimated that LOSP occurs about ten times per year per reactor [3]. However, a recent assessment of "station blackout" based on information from Licensee Event Reports (LER) indicates that the probability of LOSP is higher for some commercial nuclear power plants [6]. Site-specific investigations reveal that the frequency of LOSP varies for different locales. Regardless of the random occurrence of LOSP, the reliability of the emergency power system (EPS) to perform its mission has to be adequately analyzed to assess the safety implications of this anticipated transient. Vesely [7] pointed out that risk analysis must be performed in conjunction with data analysis to provide pertinent reliability and safety information for decision-making in the nuclear licensing process.

The availability of the emergency onsite power supply to the ESF loads within thirty (30) seconds after LOSP is essential to mitigate the progression and consequences of a core melt initiated by this transient. Chu and Gaver [8] derived and evaluated the long-term system availability of single-unit and triple-unit standby systems by stochastic process methods that involved a linking of two Markov processes. The optimum inspection interval for enhanced system availability was examined. Pages et al. [9] evaluated the reliability and availability of large repairable systems by the method of critical running states. Azarm et al. [10] showed that availability of the emergency onsite power system can be estimated by dynamic Markov modeling techniques. Vaurio [11] developed comprehensive availability models for analyzing redundant standby safety systems. These models provide techniques for obtaining optimum test

intervals for improvement in system availability. Mankamo and Pulkkinen [12] established that the availability of the emergency power system, viz., the diesel generators, depends on the test intervals.

Since the dc power supply is an integral part of the EPS, the nuclear power plant is required to enter into a shutdown mode when there is a failure of one dc bus in the plant electrical distribution system. It was postulated that the sudden gross failure of redundant dc power supplies during normal plant operation could lead to insufficient shutdown cooling of the reactor core. Eisenhut [13] utilized a probabilistic approach to evaluate the reliability of dc power supplies in a nuclear power plant. The study concluded that the likelihood of dc power supply failures leading to insufficient shutdown cooling of the reactor core was sufficiently small ($<10^{-6}$ per reactor year) so that no further consideration was required. Even though the failure of dc power supplies represented a small contribution to the probability of a core-melt accident, dc power-dependent failures involving decay heat removal system and reactor coolant system integrity are nevertheless potentially significant for certain plant designs [14].

In the quantified reliability analysis of a complex system such as the EPS, common mode failures (CMF) or common cause failures (CCF) can be a significant and difficult aspect. Fleming and Raabe [15] compared three methods to predict the reliability characteristics of redundant systems subject to independent and common cause failures. Markov modeling showed that the beta factor statistics used in the High Temperature Gas-Cooled Reactor risk assessment study was consistent with the Marshall-

Olkin approach based on the multivariate exponential distribution. The reliability for diesel generator startup as calculated by the beta factor statistics was consistent with the result from the geometric mean approach used in the RSS. Easterling [16] had attempted to define CMF or CCF by a probability model dealing with dependence among failure events, dependence of failure events on the conditions under which an item is designed to perform, and dependence among these conditions. The probability model was used to investigate the adequacy of bounds on the probability of multiple failures. Steverson and Atwood [17] used the binomial distribution model to estimate the common cause failure rates for diesel generators in nuclear power plants based on LERs from 1976 to 1978. However, plant-to-plant variations complicate the calculation of these estimates. Common mode failures of redundant elements in the design of nuclear systems have been a major concern to the Advisory Committee on Reactor Safeguards (ACRS) over the years [4]. This concern had guided the ACRS to recommend appropriate modifications of nuclear plant designs to account for systematic (common mode or common cause) failures.

The Three Mile Island-2 accident showed that inadequate attention in design, analysis and operations may have been given to complex transients, small LOCAs and reliable decay heat removal [5]. The accident demonstrated the importance of comprehensive analyses of strategies or options so as to preclude initiation of transients and to avoid consequences that may lead to core melt. The response of a PWR to a hypothetical meltdown sequence initiated by loss of offsite and onsite power and auxiliary feedwater had been qualitatively analyzed by Haskin et al. [18]. The core

meltdown, containment response and consequences to the public have been dealt with in a deterministic manner. However, the probability of the accident occurring was not computed and the risks associated with the plant response were not quantified.

The overall system safety and performance in nuclear power plants can be improved by using probabilistic methodology to search for potential weak points in the designs of nuclear generating stations in operation or under construction. Fussell et al. [19] outlined a computer-aided methodology to determine the relative contributions of various subsystems and components to the total risk associated with an engineered system. The major contributors to system risk were identified through comparison of expected frequency distribution functions with an established risk criterion. The critical subsystems, components and failure modes that affect plant availability can be identified. However, this also requires an overall system knowledge and the engineering judgment to examine the basic system operation in a critical manner [20].

Finally, other risk analyses of light water reactor plants are continuously being performed to examine the full spectrum of accident initiators. The German Risk Study is quantitatively evaluating the contributions of additional initiating events that had not been considered in the RSS [21].

IV. RELIABILITY ASSESSMENT METHODOLOGY

All systems eventually fail because nothing is perfectly reliable. System failure can occur in many ways, and it involves single or multiple component failures. The degradation of a multicomponent system can be properly assessed from the reliability of its components to perform their desired missions.

The probability density for failure of a component can be described by a function f(t). The cumulative probability for failure, F(t), is related to the probability density for failure by the equation [3, 22]

$$F(t) = \int_0^t f(t)\, dt \tag{4.1}$$

Differentiating with respect to t,

$$f(t) = \frac{dF(t)}{dt} \tag{4.2}$$

For systems in continuous operation, the failure intensity rate (or hazard rate) is defined by [3, 23]

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \tag{4.3}$$

Substituting Eq. 4.2 into Eq. 4.3.,

$$\lambda(t) = \frac{dF(t)/dt}{1 - F(t)} = -\frac{d}{dt}\{\ln [1 - F(t)]\} \tag{4.4}$$

Integrating with respect to t,

$$\ln [1 - F(t)] = -\int_0^t \lambda(t)\, dt \tag{4.5}$$

Therefore,

$$1 - F(t) = \exp\left[-\int_0^t \lambda(t)\, dt\right] \tag{4.6}$$

Reliability R(t) is the probability that a system performs a specified function or mission under given conditions for a prescribed time. It defines the probability that a system or device will not fail during a time period t [3]. Hence, it is the complementary probability to F(t), i.e.,

$$R(t) = 1 - F(t) \tag{4.7}$$

From Eq. 4.6,

$$R(t) = \exp\left[-\int_0^t \lambda(t)\, dt\right] \tag{4.8}$$

Assuming that failures are uniformly random events that are mutually independent, the failure intensity rate becomes constant such that [3]

$$\lambda(t) = \lambda \tag{4.9}$$

If the components in a system have random failure rates, λ_i, then the ith component reliability is simply

$$R_i(t) = e^{-\lambda_i t} \tag{4.10}$$

A. System Reliability Block Diagram

System reliability can be predicted by the representation of the active components in a reliability block diagram (RBD) that portrays the

successful pathway of system functions or operation. The RBD is a model of statistically independent components that operate in series or in active-parallel. It is generated by an inductive process that identifies all pathways for system success.

A series configuration of N components in a system is shown in Figure 1. If each of the N independent units has reliability R_n, the reliability of the system structure is described by the general equation [3, 23]

$$R_s(t) = \prod_{n=1}^{N} R_n(t) \tag{4.11}$$

If each component exhibits a constant hazard, then

$$R_s(t) = \prod_{n=1}^{N} e^{-\lambda_n t} = \exp\left[-\sum_{n=1}^{N} \lambda_n t\right] \tag{4.12}$$

If a system of n components can function properly when only one of the components is operable, a parallel configuration is indicated. A parallel configuration of N components is shown in Figure 2. The reliability function for an active-parallel system is generally expressed as [3, 23]

$$R_p(t) = 1 - \prod_{n=1}^{N} [1 - R_n(t)] \tag{4.13}$$

Reliability block diagrams have been used in the probabilistic risk assessment of nuclear plants to facilitate the quantification of system fault trees.

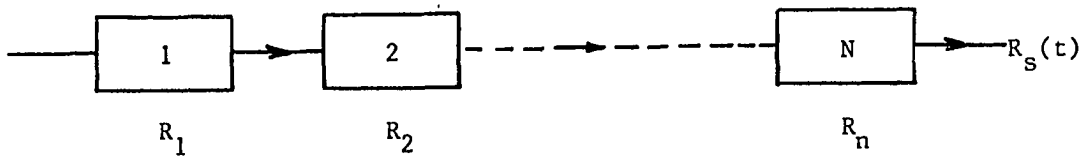


Figure 1. Series configuration in a reliability block diagram

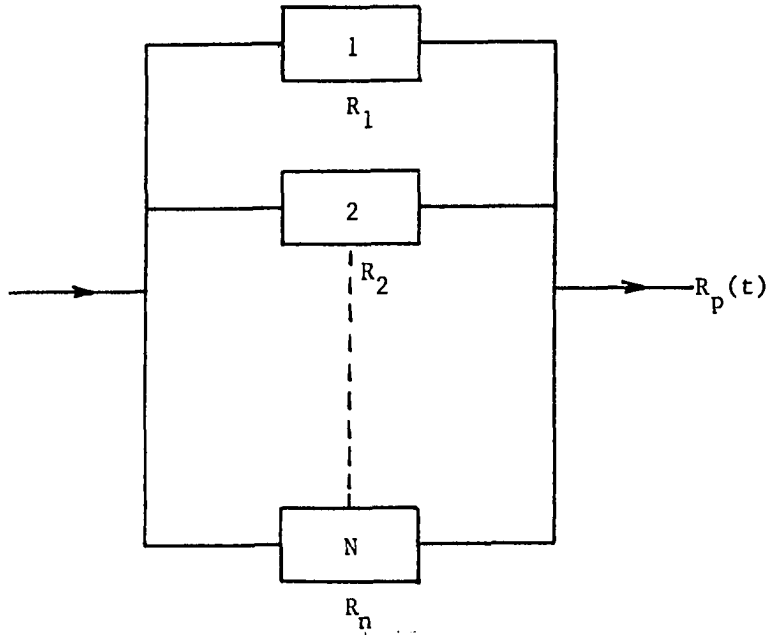


Figure 2. Parallel configuration in a reliability block diagram

B. System Availability

The system instantaneous availability A(t) is the probability that a system performs a specified function or mission under given conditions at a prescribed time. The probability 1 - A(t) is termed the instantaneous unavailability. The instantaneous availability is bounded such that

$$R(t) \leq A(t) \leq 1 \tag{4.14}$$

For a nonrepairable system, the system unreliability or unavailability is q [3]:

$$\begin{aligned} q &= 1 - R(t) \\ &= 1 - e^{-\lambda T} \end{aligned} \tag{4.14}$$

where λ is the constant hazard rate for a device that experiences random failures and T is the mission time of interest. For small values of λT (< 0.1), the system unavailability, q is approximated such that [1, 3]

$$q \doteq \lambda T \tag{4.16}$$

The overall system unavailability can be computed from a system fault tree that analyzes the possible mechanisms of failure. The failure mechanisms in a system are logically represented as fault events on the fault tree structure. The fault events are pictorially combined to show their causal relationships to an undesired (top) event. Since unavailability is the probability of being in a failed state at any given time, the occurrence probability of a basic fault event represents the unavailability of a system component with a constant failure rate [1]. There-

fore, system unavailability can be evaluated from a quantitative assessment of a fault tree.

C. Fault Tree Process

Quantitative analysis of the fault tree consists of transforming its established logical structure into an equivalent form and numerically calculating the occurrence probability of the top event from the occurrence probabilities of the basic events. The occurrence probability of the top event can be evaluated by the solution of Boolean algebraic equations for the gates of the system fault tree. For each gate of the tree, the input events (such as the primary events) are the independent variables, and the output event (such as the intermediate event) is the dependent variable. The probability of the output event can be computed by applying the Boolean expressions to the basic gates, AND gate and OR gate, of the tree.

For n inputs to the AND gate, the probability of the top event is expressed by the equation [3]

$$P(A_1A_2\cdots\cdots\cdots A_N) = P(A_1)\ P(A_2)\cdots\cdots\cdots P(A_N) \tag{4.17}$$

In the case of the OR gate with n inputs, the probability expression for the top event is given by [3]

$$P(A_1+A_2+\cdots\cdots+A_N) = \sum_{n=1}^{N} P(A_n) - \sum_{n=1}^{N-1}\sum_{m=n+1}^{N} P(A_nA_m) + \cdots + (-1)^{N-1} P(A_1A_2\cdots A_N) \tag{4.18}$$

Since the basic event probabilities, $P(A_n)$, are normally very small, the Boolean expression for the OR gate with n statistically independent inputs is often represented by the approximation [3]

$$P(A_1+A_2+\cdots+A_N) \doteq \sum_{n=1}^{N} P(A_n) \tag{4.19}$$

The resulting probability from each calculation for a logic gate is used as an input to the calculation of the event corresponding to the next gate higher in the fault tree. In this manner, the probability of the top event can be quantified in terms of the minimum number of basic events from the bottom to the top of the tree.

Table 1 shows the symbols commonly used in the construction of a fault tree. Figure 3 shows the Boolean operation involved in the quantification of a typical fault tree. Table 2 provides the specifications for this fault tree.

For the typical fault tree example, the primary fault events, B, C, D and E are inputs to the OR gates T_3 and T_4. The inputs to the AND gate T_2 are the intermediate fault events T_3 and T_4. The top event T_1 is an OR gate combination of primary event A and the intermediate fault event T_2. Hence, the probability of the top event is computed as

$$P(T_1) = P(A) + P(T_2) \tag{4.20}$$

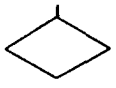
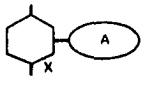
where

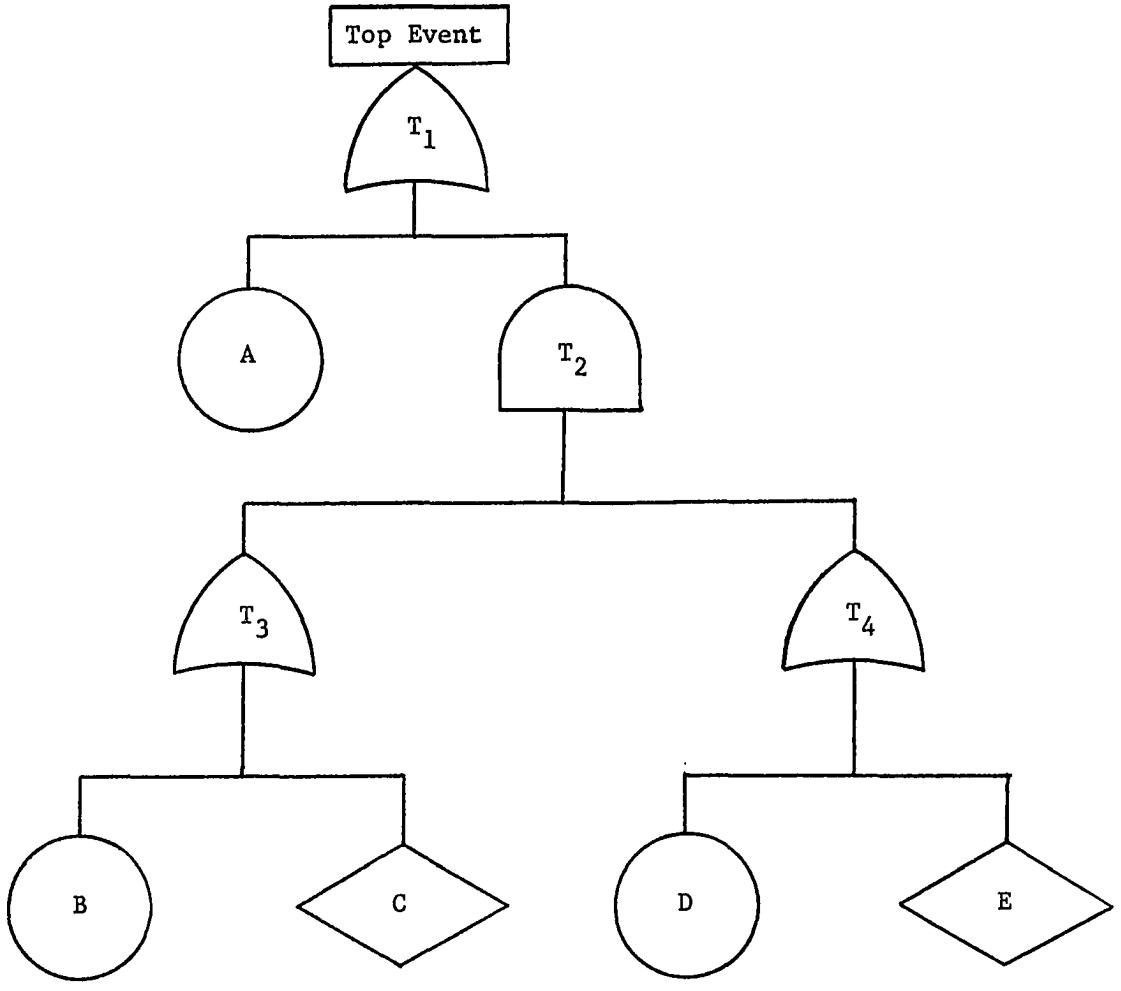
$$P(T_2) = P(T_3) \cdot P(T_4)$$

$$P(T_3) = P(B) + P(C)$$

$$P(T_4) = P(D) + P(E)$$

Table 1. Common fault tree symbols

Symbol	Name	Description
	Rectangle	Fault event; it is usually the result of the logical combination of other events
	Circle	Independent primary fault event.
	Diamond	Fault event not fully developed as to its causes; it is only an assumed primary fault event.
	House	Normally occurring basic event; it is not a fault event.
	OR Gate	The union operation of events; i.e., the output event occurs if one or more of the inputs occur.
	AND Gate	The intersection operation of events; i.e., the output event occurs if and only if all the inputs occur.
	INHIBIT Gate	Output exists when X exists and condition A is present; this gate functions somewhat like an AND gate and is used for a secondary fault event X.
	Triangle-In	Triangle symbols transfer the tree construction from one sheet to the next. The triangle-in appears at the bottom of a tree and represents that branch of the tree ("A") shown someplace else. The triangle-out appears at the top of a tree and denotes that the tree "A" is a subtree to one shown someplace else.
	Triangle-out	



$$T_1 = A + T_2$$

$$T_2 = T_3 \cdot T_4$$

$$T_3 = B + C$$

$$T_4 = D + E$$

Figure 3. Boolean process for quantification of a fault tree

Table 2. Specifications for the typical fault tree

Gate	Type	Inputs
T_1	OR	A, T_2
T_2	AND	T_3, T_4
T_3	OR	B, C
T_4	OR	D, E

D. Event Tree

A fault tree analysis is used to calculate the conditional probabilities needed for each branch of an event tree that identifies the various outcomes of a given initiating event. Any path from the initiating event to a final outcome is called an accident sequence. The event tree facilitates the systematic description of possible success and failure states that evolve from an event initiator. In an event tree, either systems or functions can serve as event-tree headings that represent the possibilities or strategies to mitigate the consequences of the initiator. A simple event tree is illustrated in Figure 4.

A type of functional event tree is the "operator action" event tree (OAET). The OAET incorporates human reliability analysis at the system event-tree level in modeling the response to a transient. It addresses the unique role of the operator in the actions to mitigate the effects of an undesirable event. The identification of automatic responses to an initiator in the OAET provides valuable information for the correct diagnosis and interpretation of key symptoms in accident initiation and progression analysis (AIPA).

E. Summary

The quantitative assessment techniques presented above is applied to the evaluation of the reliability of the emergency power system described in the following section. The major active components in the electrical

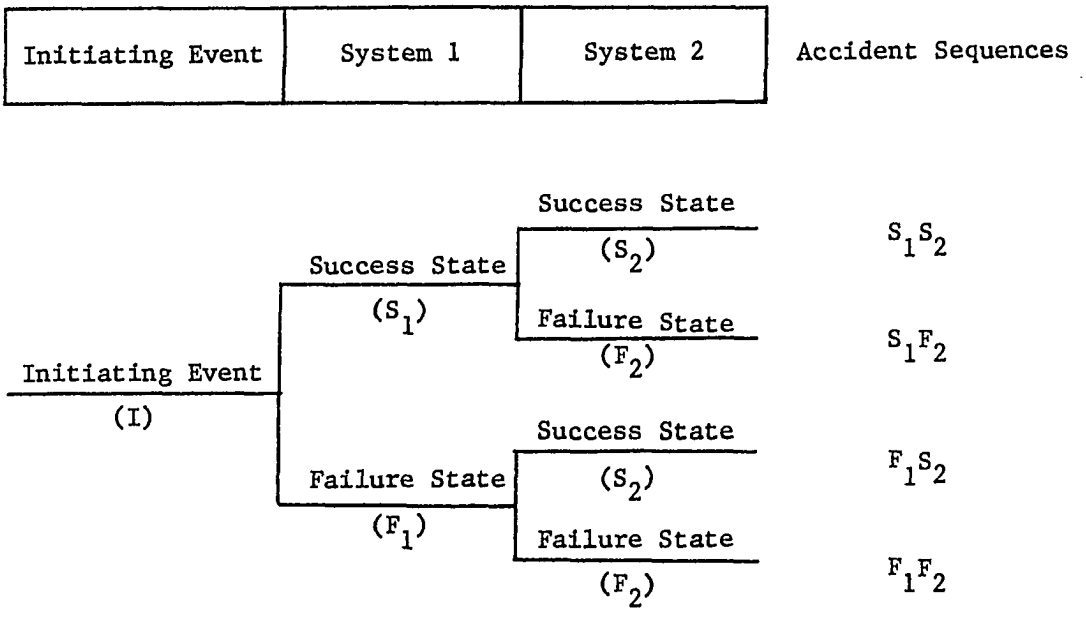


Figure 4. A simple event tree

power distribution system that operate during normal plant operation are independent units whose individual random failure may affect the total system reliability. Since the components have constant failure rates, system unreliability from hardware failures only can be effectively analyzed by a RBD model. The RBD method structures the various devices in series into "supercomponent trains" and then links together the parallel supercomponents to form a summary model of the system design. The quantitative assessment of system reliability then involves the application of the appropriate general reliability equations for the series or active-parallel configurations in the RBD.

During normal plant operation, there may be off-normal events that interact to produce other events to cause system unavailability. The possible combinations of fault events associated with the mission of the emergency power system can be analyzed by fault tree methodology. The fault tree analysis includes human interactions and initial system conditions in addition to hardware failures. Using updated failure data for the basic events that result in the occurrence of the undesired event, i.e., insufficient power to the 4.16-kV engineered safety feature bus, the quantitative evaluation of system unavailability is performed.

An abnormal event such as loss of offsite power affects the availability of the emergency power system in a nuclear power plant to provide adequate power to the engineered safety systems. The progression of this event and the automatic plant responses can be investigated by an event tree. The influence of human actions to mitigate the consequences of the

transient event is addressed in the OAET. This methodology provides the structure for probabilistic analysis of human factors in the event.

V. THE ELECTRIC POWER SYSTEM

Electrical power is required for the normal operation of the various systems in a nuclear power plant. These systems generally consist of the Nuclear Steam Supply system and the Balance of the Plant system. The electrical power distribution system in the nuclear power facility should provide a means for the reliable supply of power to all components in the systems. The distribution network supplies power from dependable sources to the equipment that must be energized for startup, normal operation and shutdown of the plant. The design of a plant electrical power distribution system includes an onsite ac power source as well as an external power source to enhance the reliability of power supply to the various plant loads.

In a typical nuclear power plant, the power sources are physically and electrically isolated to the maximum extent so that any single failure will affect only one source of supply. Since a reliable power supply is vital for operation of the plant systems, total loss of ac power from all supply sources (station blackout) has a direct impact upon the plant operational safety. Furthermore, a station blackout results in a sudden loss of nuclear electrical generation. Therefore, the occurrence of total station blackout must be minimized.

The basic components in the electrical power distribution system are a main generator, main transformers, unit auxiliary transformers, startup transformers, station service transformers and dc power sources. These devices are all directly connected in a unique configuration to provide

reliable service to the plant loads. Standby diesel generators supply emergency power in the event of a complete loss of normal external ac power.

Figure 5 shows a simplified one-line diagram of the electrical power distribution system for a typical 1100 MW(e) pressurized water reactor power plant of the Combustion Engineering design. The bus designations in the electrical distribution system are provided in Table 3.

Table 3. Bus designations in the electrical power distribution system

Voltage	Buses
6.9 kV	1A, 1B
4.16 kV (Nonsafety)	2A, 2B, 4A, 4B
4.16 kV (Safety)	3AS, 3BS, 3ABS
480 V (Nonsafety)	21A, 21B, 22A, 22B, 32A, 32B
480 V (Safety)	31AS, 31BS, 31ABS

The electrical power system for this particular nuclear generating station (Waterford 3) consists of an onsite ac power system and dc power system [24, 25]. The ac power system provides electrical energy to operate the mechanical equipment in the plant systems. The dc power system provides uninterruptible 125-V dc power for instrumentation and control systems.

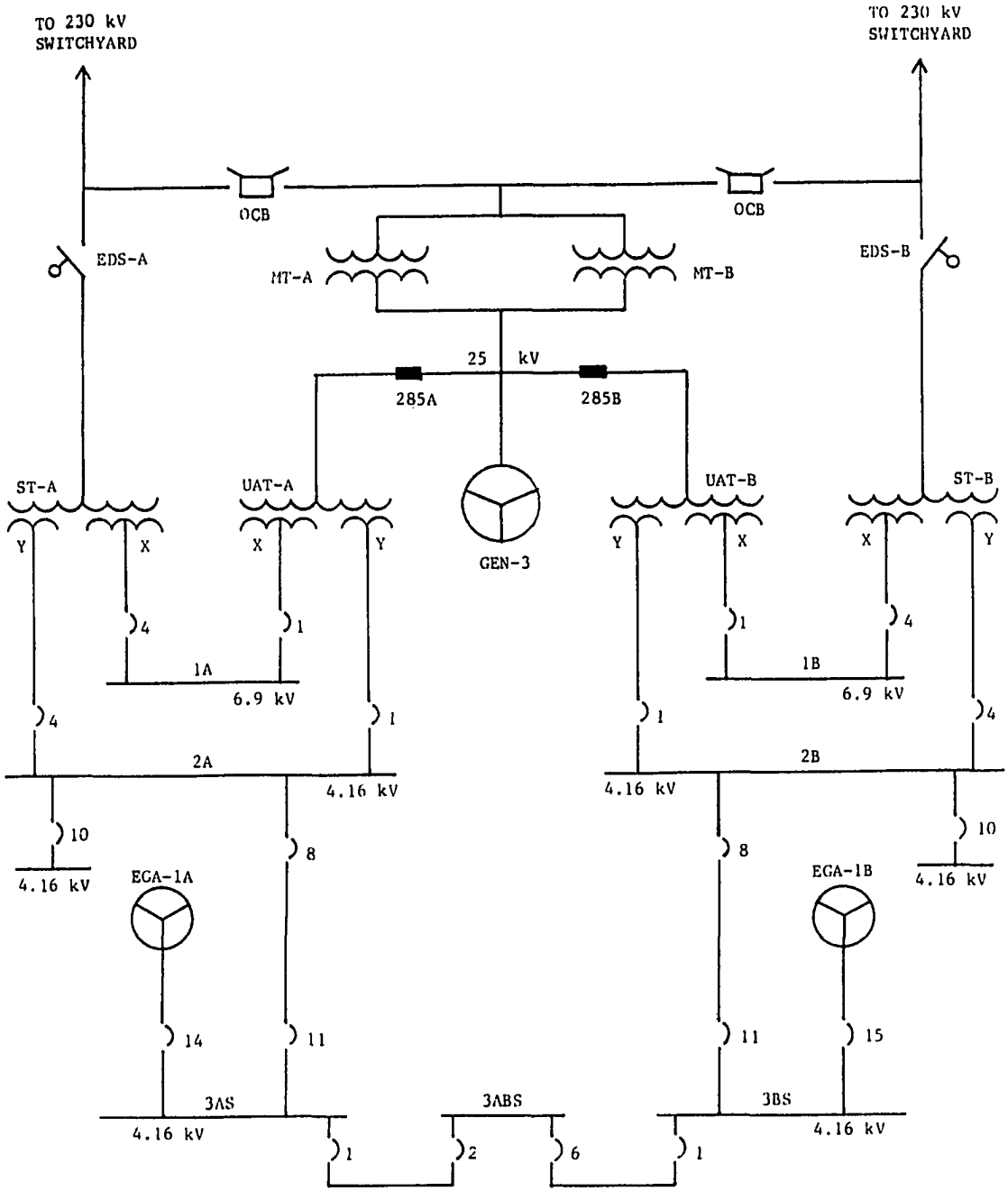


Figure 5. A single-line diagram of the electrical power distribution system

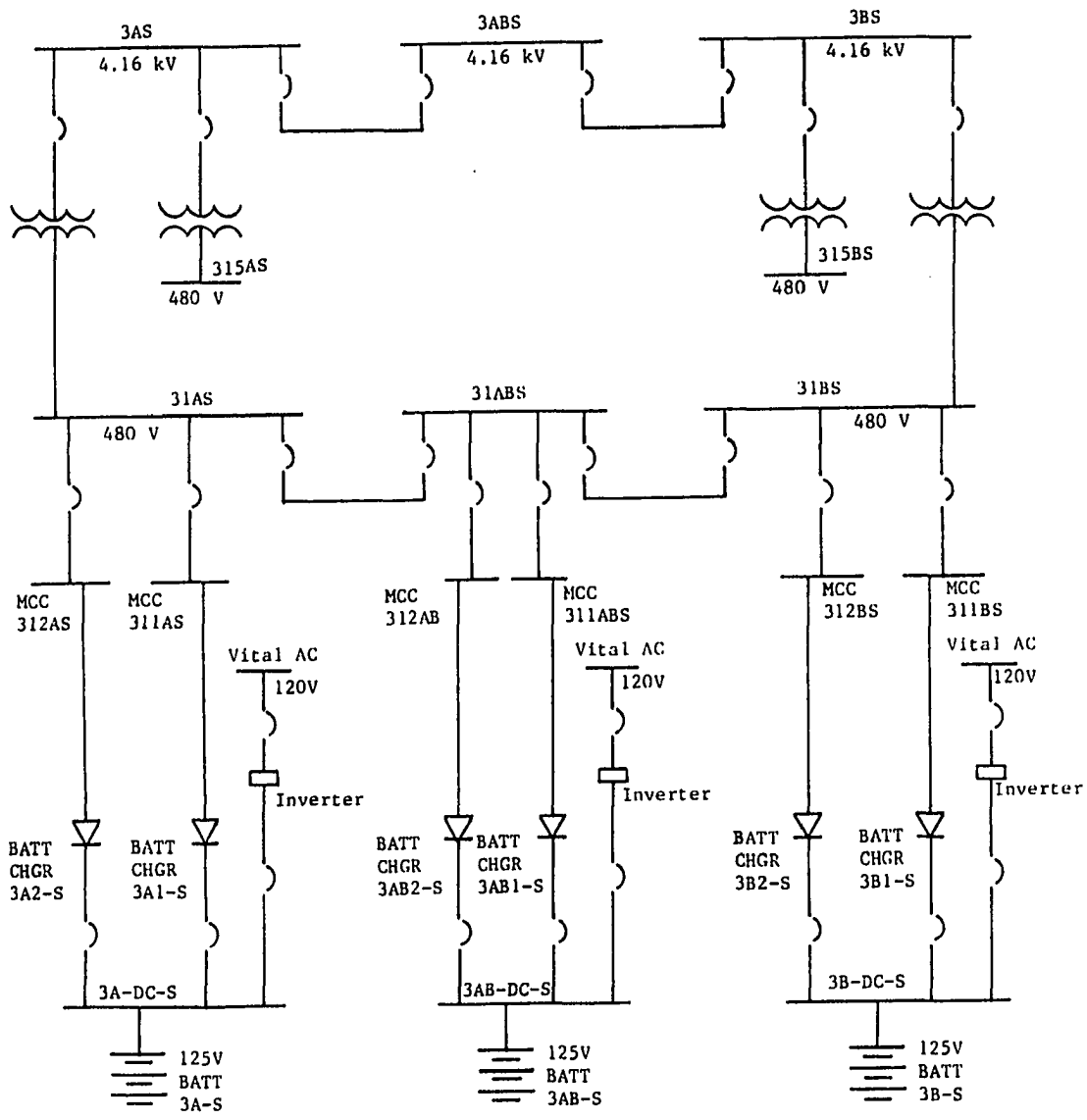


Figure 5. (Continued)

A. Onsite ac Power

The onsite ac power distribution system consists of two redundant, and basically independent trains, Train A and Train B. Each train is a network of feeders from the power sources and electrical buses dedicated to serve their associated loads. The two trains are isolated (except for interconnections between buses on separate networks) so that any single failure affects one network only. The ac power distribution system consists of the following major subsystems:

1. Transformers and switching station
2. 6.9-kV electrical distribution
3. 4.16-kV electrical distribution
4. 480-V electrical distribution
5. 120-V vital ac
6. Emergency diesel generators

1. Transformers and switching station

The transformers and switching station subsystem provides a means for transmitting the station output to the utility grid. This subsystem provides two electrically and physically independent, redundant and reliable transmission circuits from the grid to the plant electrical distribution system.

For this particular power plant, the switching station connects the plant to a HV switchyard by means of two, 230-kV transmission lines. Each line is on an independent structure sharing a common right of way. The switching station contains a structure for terminating the two trans-

mission lines, two motor-operated disconnect switches, two oil circuit breakers (OCB) and interconnecting bus and supporting structures.

The transformer yard contains the two main transformers (MT-A and MT-B), the two startup transformers (ST-A and ST-B), the two unit auxiliary transformers (UAT-A and UAT-B), connecting buses and overhead lines. The main transformers are each half load, delta-wye connected, shell form transformers that step up the output voltage of the main generator (GEN-3) from 25 kV to 230 kV. Each main transformer is rated at 600 MVA, 3 phase, 60 Hz and is of the forced oil-to-air (FOA) cooled type. The two startup transformers are 33.6/44.8/56 MVA, wye-delta connected, core form transformers that step down the grid voltage from 230 kV to 7.2 kV and 4.36 kV for in-plant loads. Each startup transformer supplies its X windings at 7.2 kV, 21.6/28.8/36 MVA and its Y windings are 4.36 kV, 12/16/20 MVA. The two startup transformers are connected to the switching station through the motor-operated disconnects (EDS-A and EDS-B).

The two unit auxiliary transformers are connected through isolated phase taps to the main bus of the generator. These are 39/52 MVA, delta-delta connected, sealed tank transformers that step down the generator output from 25 kV to 6.9 kV and 4.16 kV for in-plant loads. Each unit auxiliary transformer supplies its X windings at 6.9 kV, 24/32 MVA and its Y windings at 4.16 kV, 15/20 MVA. An isolated phase bus is used to connect the generator to the low voltage bushings of the main transformers.

The main transformers are connected in parallel through an isolated phase bus, which is connected in turn to the main generator bus. Isolated phase taps are used to connect the unit auxiliary transformers to the

generator bus. The eight medium voltage (secondary) transformer windings (two each for the two startup and the two unit auxiliary transformers) are connected to the plant electrical distribution system switchgear through cable bus ducts.

During normal operation, the transformers and switching station are in a fixed lineup. The most dynamic time for this subsystem is during shutdown or startup operations when transfers to and from the startup transformers take place. While the plant electrical distribution system is being supplied from the unit auxiliary transformers, the startup transformers are in a standby condition. If the main generator fails, the output breakers (OCB S7120 and S7130) will open and the plant loads would be shifted automatically to the startup transformers. The transformer cooling systems are aligned with one group selected as a lead cooling unit and the other group as a standby cooling unit. As winding temperature increases, the lead cooling group starts. The standby cooling group will start if the temperature increases to a higher temperature.

2. 6.9-kV electrical distribution

The 6.9-kV electrical distribution subsystem supplies power to the major motors (4000 hp and above) in the plant that are not safety-related. This subsystem is operable as long as the main generator or the 230-kV grid are in service. Unless the 6.9-kV subsystem is removed from service for maintenance, power will be available to the major motors all the time.

The 6.9-kV electrical distribution subsystem originates at the X windings of the startup and the unit auxiliary transformers. The subsystem receives power from the main generator through the unit auxiliary

transformers during normal conditions or from the startup transformers when the main generator is in the shutdown mode. Both transformers supply 6.9-kV nominal power to the buses. The 6.9-kV switchgear distributes the power received from the transformers to the 6.9-kV motors. There are two buses, 1A and 1B, which connect the power to the individual motor feeder breakers. The 6.9-kV motors that receive power from these two buses are the 4 reactor coolant pumps (RCP), 4 circulating water pumps (CWP) and 3 condensate pumps (CP).

During plant startup, ac power from the 230-kV grid is transformed into 6.9-kV power by the startup transformers. Once the main generator is on-line, the power supplied to the redundant 6.9-kV buses (1A and 1B) from the startup transformers is transferred to the unit auxiliary transformers. After the transfer is complete, the main supply breakers (1) are interlocked so that only one source of power is supplying the bus. If the power supply from the unit auxiliary transformer is lost, the supply will shift to the startup tranformer. The failure of either 6.9-kV bus will result in a trip of the reactor by the reactor protection system (low flow).

When power is supplied to the buses, the operator can close feeder breakers to the various motors as needed. Protective relaying is provided as a means of preventing excessive damage to components from electrical faults. Undervoltage relays in the switchgear assembly will trip all feeder breakers on loss of power to the bus. These undervoltage relays are connected to potential transformers that reduce the 6.9-kV bus voltage to 115 V for safety and for the use of indication and control equipment.

Overcurrent relays will trip incoming breakers if excessive current flows due to a faulted bus or an outgoing feeder breaker fails to trip when there is a fault on the feeder.

3. 4.16-kV electrical distribution

The 4.16-kV electrical distribution subsystem provides power to all the plant loads with the exception of motors that have horsepowers of 3000 or greater. This subsystem is required during normal plant operations, startup and shutdown conditions and in emergency situations. During normal conditions, power is supplied from the transformers and distributed throughout the plant by this subsystem. If offsite power is lost, the vital plant loads are supplied from emergency diesel generators.

The 4.16-kV electrical distribution subsystem consists of four buses (two divisions) of nonvital loads and three buses (three divisions) of vital loads. Normally, the nonvital divisions supply the vital divisions with power. The divisions are separated into two major groups such that a single major fault will not jeopardize the plant.

The two vital divisions are protected from any loss of power by the emergency diesel generators. The third vital division receives its power from one of the other two vital divisions. However, this bus (3ABS) cannot receive power from both buses simultaneously. This bus supplies power to equipment that is standby to equipment on the other buses. Either major vital bus can supply sufficient power to shut down the plant and mitigate core damage. Each of the 4.16-kV buses further provide power supply to transformers that reduce the voltage for operating equipment that require lower voltage.

The major components associated with the 4.16-kV electrical distribution subsystem are as follows:

- 4.16-kV switchgear
- buses 2A and 2B
- buses 4A and 4B
- buses 3AS and 3BS
- bus 3ABS
- cable bus duct
- nonsegregated phase bus duct
- cable feeders

The normal plant electrical distribution system is supplied by four nonsafety-related switchgear assemblies. In addition, the three safety-related switchgear assemblies receive power from the normal distribution system or from the emergency diesel generators. The electrical buses 2A and 2B supply 4.16-kV motors, station service transformers, nonsafety buses 4A and 4B, and safety buses 3AS and 3BS. Each bus (2A or 2B) is supplied from its own startup and unit auxiliary transformers through an incoming line breaker (1 and 4). The two incoming breakers (1 and 4) are interlocked so that only one transformer can supply the bus at a time. The supply for these buses would automatically transfer to the startup transformer if the unit auxiliary transformer fails, or the main generator trips.

The buses 4A and 4B are supplied from buses 2A and 2B, and they serve the supplementary water chiller area. The incoming feeders are connected directly to the bus without circuit breakers. The feeder breakers in buses 2A and 2B provide for bus protection. The feeders that serve the administration building and the station service transformers are protected

by overcurrent relays and ground fault alarms. The feeders to the supplementary chillers are protected by thermal overload relays.

The safety-related motors and load centers are powered from buses 3AS and 3BS. Each bus has two incoming feeder breakers (11 and 15). One breaker connects its normal supply from the nonsafety bus and the other connects the output from the emergency diesel generator. The feeder from the nonsafety-related buses have overcurrent protection and undervoltage relays. If there is trouble in the subsystem or on the feeder, these relays will trip the breaker. These relays will also start the diesel generator and initiate a permissive loading sequence. A breaker is provided on each bus (3AS or 3BS) for supplying power to bus 3ABS. These breakers (1) have overcurrent protection but not ground fault alarms. The "installed reserve" safety-related motors are powered from bus 3ABS. This bus may be connected to either bus 3AS or 3BS, but not both at the same time. If the bus is shifted from one supply to the other, the 480-V ac power supply is also changed accordingly.

The feeders from the startup and unit auxiliary transformers to the normal supply buses, 2A and 2B, consist of 15 conducting cables (5 per phase). These cables are arranged in a steel ventilated duct with spacers between the cables. Similar cable bus ducts are used to supply buses 3AS and 3BS from buses 2A and 2B respectively. The two feeders that go to bus 3ABS and 3AS and 3BS are called nonsegregated phase bus ducts. This connection is made using rigid conductors instead of cables. The cable feeders to the loads on the nonvital buses are composed of cable in

conduit. Each feeder is a rubber-insulated, shielded conductor. The feeders consist of six conductors, two for each phase.

During generator shutdown conditions, the 4.16-kV electrical distribution subsystem is supplied from the startup transformers. The buses 2A and 2B further provide supply to buses 3AS and 3BS respectively. When the main generator is on-line, the loads are shifted to the unit auxiliary transformers. This is the normal line-up during normal plant operating conditions.

There are two basic built-in safety devices that will provide reliable in-plant power. First, if a fault causes the loss of the unit auxiliary transformers, the power loadings will be shifted to the startup transformers automatically. If further problems are encountered, i.e., a loss of offsite power, the breakers (8 and 10) between the nonvital and vital buses will open and lock out. The emergency diesel generators will start. Once these diesel generators are running, the loads will be picked up by the automatic sequencing system.

For normal plant operation, the unit auxiliary transformer supplies bus 2A. This further supplies bus 3AS and this in turn supplies other buses and transformers for in-plant loads. The same is true for bus 2B and its associated buses.

The safety-related motors supplied with power from the safety-related buses 3AS, 3BS and 3ABS are for the following:

- high pressure safety injection pumps
- low pressure safety injection pumps
- essential services water chiller compressors

- component cooling water pumps
- auxiliary component cooling water pumps
- containment spray pumps
- emergency feedwater pumps

Figure 6 shows the various equipment (safety and nonsafety) loads that are aligned to the 4.16-kV electrical buses.

4. 480-V electrical distribution

The 480-V electrical distribution subsystem provides and distributes electrical power to motors and various other lower voltage loads. It also provides power for the 480-V ac safety-related loads that are required for the safe shutdown of the plant. This subsystem is operable during start-up, normal operation, shutdown and emergency conditions. The safety-related loads are distributed in redundant groups such that the loss of one group will not affect the safe shutdown of the plant.

The 480-V electrical distribution subsystem consists of two major sections, i.e., nonvital and vital sections. All the 480-V ac power is supplied by station service transformers from the 4.16-kV electrical distribution subsystem. The nonvital section is divided into two redundant divisions. The safety-related (vital) section is also divided into two redundant divisions. There is a third safety-related division that powers the "installed reserve safety loads." This division can be fed from either safety-related division, but it cannot be connected to both at the same time. The nonvital and vital load centers distribute 480-V ac power to the larger components and the motor control centers.

The motor control centers provide power to the smaller components throughout the plant. The safety-related section is distributed into

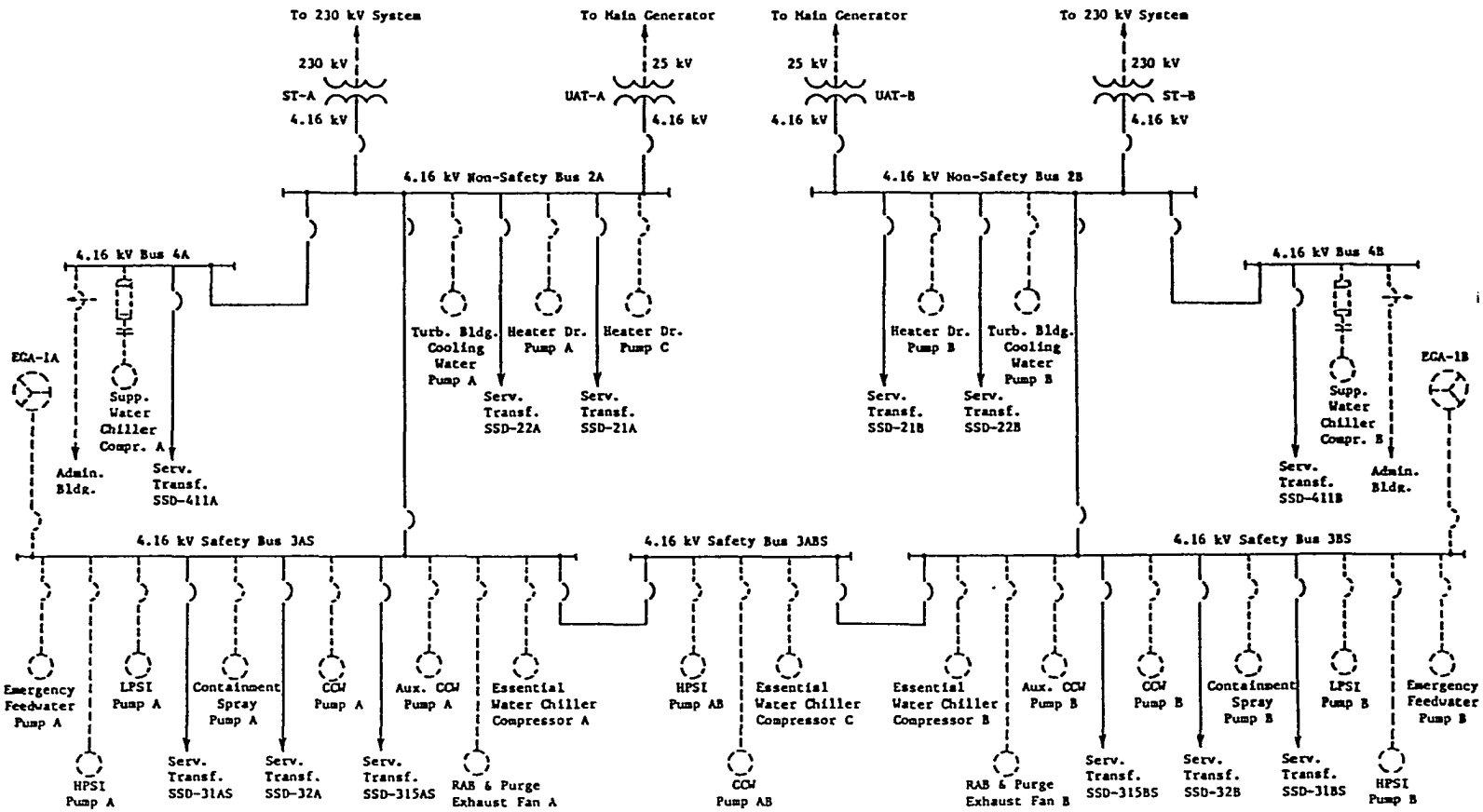


Figure 6. Electrical loads on the 4.16-kV distribution system

redundant groups with sufficient electrical and physical separation. This prevents a fire or some physical problem from causing the loss of both groups at the same time. The nonsafety sections are constructed with similar separation whenever possible.

The 480-V electrical distribution subsystem operates essentially the same in all modes of plant operation. Once the subsystem is energized, it remains fairly unchanged.

The nonvital distribution section consists of 12 station service transformers, 6 load centers and 19 motor control centers. The vital distribution section supplies the equipment necessary for emergency reactor protection and support. This section can be supplied from the offsite power system or by the emergency diesel generators. The vital section consists of 4 station service transformers, 3 load centers and 13 motor control centers. The motor control centers consist of metal-enclosed groups of motor starters and control devices. The motor starters consist of a contactor and a circuit breaker enclosed in a molded case for protection. These are called "combination starters."

5. 120-V vital ac

The 120-V vital ac subsystem provides a reliable, uninterruptible supply of 120-V ac power to the plant protection system, engineered safety feature (ESF) system and various other loads during startup and normal operation of the plant. It is also designed to provide the necessary power to those loads that are required to safely shut down and cool down the reactor under normal and emergency conditions.

The subsystem consists of seven static uninterruptible power supplies (SUPS). Six SUPS are for safety-related loads and one SUPS is for non-safety-related load. Four of the safety-related SUPS provide power for the plant protection system, including the reactor protection systems and core protection calculators, and other instrumentation and control systems that monitor and control the reactivity, temperature and other vital parameters within the reactor core. The other two safety-related SUPS (A-S and B-S) provide power for the ESF system.

The safety-related SUPS receive their normal and bypass power from 480-V safety-related motor control centers. If this supply fails, the SUPS will automatically receive power from the 125-V dc battery. The static inverter receives the regulated dc output of the rectifier (battery charger) and changes it to high quality ac. The 125-V dc battery remains in a "float" condition to automatically supply the inverter when the rectifier output becomes unavailable. The nonsafety-related SUPS (AB) provides power to other important but nonsafety-related loads.

6. Emergency diesel generators

The emergency diesel generators provide two independent onsite power sources dedicated to their respective ESF system trains. Each diesel generator is capable of providing 100 percent power requirements for its respective 4.16-kV safety bus in the event of the loss of the auxiliary transformers and the startup transformers. The diesel generators and their auxiliaries provide the emergency power for the safe shutdown of the reactor, the removal of reactor residual heat, and the maintenance of

the reactor in a safely shutdown condition upon the loss of preferred ac power.

Each diesel generator set is a complete package unit with all auxiliaries required to make it a self-sufficient power source with the capability for automatic starting and loading. The control circuits for each diesel generator operate from separate 125-V dc systems supplied from separate station batteries. The diesel generator EGA-1A is aligned to supply power to the 4.16-kV bus 3AS, and the diesel generator EGA-1B is aligned to supply power to the 4.16-kV bus 3BS. Each of the diesel generator units is rated at 4400 kW, 0.8 power factor and 4.16 kV.

The diesels are equipped with air starting mechanisms and a separate air starting system. Each diesel engine has auxiliary systems that maintain adequate engine temperature to ensure fast starts. These systems include a jacket water heater and a lubricating oil heater. Cooling water to the diesel generator jacket water heat exchangers is supplied from the component cooling water system (CCWS).

Each diesel generator can be started automatically by either a safety injection actuation signal (SIAS) or by the undervoltage relays on the respective 4.16-kV safety buses. If both diesel generators are available, both will start automatically upon receipt of the SIAS. If the undervoltage relays for the safety buses sense a "dead" bus, the associated diesel generator will be automatically started and connected to its respective bus. After the automatic start, each diesel generator unit attains rated speed and rated voltage within 6 seconds and automatically accepts loads in sequence as well as subsequent manually-applied loads. Each diesel

engine is a 16-cylinder, V-type, turbocharged, 4-stroke engine. The rated speed of the engine is 600 rpm. The engine trips on overspeed at 660 rpm and also on generator differential.

The major components in each diesel generator unit are:

- diesel engine
- emergency diesel lube oil system
- emergency diesel cooling system
- emergency diesel generator air system
- emergency diesel fuel system
- generator

B. Onsite Uninterruptible dc Power

The onsite dc power distribution system consists of three batteries and related auxiliaries. The dc power system provides uninterruptible 125-V dc power continuously to specific loads that are required for the safe operation and shutdown of the reactor plant. The system also supplies power to control systems, instrumentation systems and other operationally essential loads. These loads include valve solenoids, control circuit relays and dc motors that operate essential backup components. During emergency operations, the system provides power to safety-related loads, essential nonsafety-related loads and the nonsafety uninterruptible 120-V ac power system.

The dc system consists of three 125-V batteries with each having its own battery chargers, dc load center and distribution panels. Each

battery is a bank of 60 lead-acid cells and is rated 1200 amp-hour for an eight-hour rate, or 600 amp-hour for one-hour rate of discharge of 1.75 volts per cell at 25° C. The three batteries, designated 3A-S, 3B-S and 3AB-S, and their associated load centers and distribution panels have been arranged to feed the safety-related redundant dc loads and the nonsafety-related loads associated with divisions A, B and AB. The batteries float on their respective buses. The battery chargers convert the 480-V ac input power to dc by means of a rectifier unit consisting of silicon-controlled rectifiers and silicon diodes. The battery chargers also provide power supply to the normal dc load on the buses. A blocking diode prevents the dc batteries from backfeeding into the dc rectifier of the inverter.

Each battery supply is continuously available during normal and emergency operation. The batteries are maintained in a fully charged condition and have sufficient stored energy to operate all necessary circuit breakers. They also provide an adequate amount of energy for all the required emergency loads. The battery chargers for one component subsystem are independent of the battery chargers of the other subsystems. Each battery charger has an input ac and output dc circuit breaker for isolation of the charger. Each battery charger is designed to prevent the ac supply from becoming a load on the battery due to a power feedback as the result of a loss of ac power to the chargers.

C. Summary

The above description of the major subsystems provides comprehensive information about the functions and basic operation of the electrical power distribution system. This information is required to facilitate evaluation of system reliability that includes causal events in a probabilistic risk assessment effort. Since each subsystem is an integral part of the electric power distribution system, component failures in a subsystem contribute to the total system unavailability. Hence, each subsystem may be qualitatively examined to identify potential contributions to system unavailability.

The emergency power system is one of the vital portions of the electrical power distribution system. An adequate supply of auxiliary power to the engineered safety systems in a nuclear power plant in the event of abnormal conditions is required to bring the station to a safe shutdown. Therefore, a systematic approach to evaluating the reliability of the electrical power distribution system is important.

The techniques in reliability assessment methodology presented in the previous chapter could be applied to evaluate the overall reliability of any electrical power distribution system. These techniques are the reliability block diagram model and the fault tree process. The unavailability of the 4.16-kV safety bus to provide adequate power to the engineered safety feature systems during an abnormal event in a nuclear power plant is analyzed by these techniques in the following section.

VI. SYSTEM RELIABILITY ANALYSIS

The emergency power system (EPS) is a vital portion of the electrical power distribution system. This system consists of: two sources of off-site ac power (the preferred source), two sources of onsite ac power (the emergency diesel generators), three sources of dc power (three 125-V batteries), and auxiliary equipment such as station service transformers, buses and cables for the distribution of power to the engineered safety feature (ESF) systems. The EPS originates at the high voltage switchyard and terminates at the 4.16-kV ESF buses (3AS, 3BS or 3ABS). Each 4.16-kV ESF bus supplies power to the vital plant loads, e.g., pumps and other equipment in safety-related systems, during emergency situations.

The principal function of the EPS is to provide adequate power to the ESF loads to mitigate the effects of probable operational incidents. Since the 4.16-kV ESF buses are the backbone buses of the EPS, the reliability of this system to ensure sufficient ESF system operability during the course of an incident is evaluated at any of the buses, 3AS or 3BS. Therefore, "insufficient power on a 4.16-kV ESF bus" describes the conditions of bus unavailability to perform its mission.

The reliability analysis for the EPS depends on failure data for the major components associated with the distribution of adequate power to each 4.16-kV ESF bus. The system reliability can be evaluated by an equation based on the reliability block diagram (RBD) drawn for the hardware associated with the EPS mission. The RBD is generated from the simplified system-success pathway for the basic operation of any system.

A. Failure Data

The failure data for the major components in the emergency power system consist of two predominant types:

1. Operating failure rate (λ_0) which denotes the probability of failure of the component to operate or function for a period of time, generally per hour.
2. Demand probability (Q_d) which denotes the probability that the component fails upon demand to operate, start or change a state or function at the time of an incident.

Table 4 provides the data for electrical equipment failure from the basic failure modes associated with each component. The data are utilized for the quantitative assessment of system reliability or unavailability on a point-estimate basis.

The failure rate for the main generator was assessed from monthly data of forced outages for U.S. nuclear power plants in commercial operation from January 1980 to November 1982 [26]. A forced outage is the loss of electrical power on a main generator tripout from some off-normal plant condition. The monthly data of forced outages are shown in the Appendix. These data provided the basis for estimating the average forced outage per operating unit in a month as 0.862. This value was used in estimating the failure (tripout) rate of main generator as 1.159×10^{-3}/hr based on 31 days in a month. The failure data for the other equipment were extracted from the Appendix III of the Reactor Safety Study.

Table 4. Failure Rates (λ_0) and demand failure probabilities (Q_d) for the basic components in the reliability block diagram

Component	Failure Mode	Computational Median
Main Generator	Trip Out	1.159×10^{-3}/hr
UAT Disconnect 285A	Fail Open	1×10^{-6}/hr
Transformer UAT-A	Short Circuit	1×10^{-6}/hr
Feeder Breaker 1-2A	Trip Open	1×10^{-6}/hr
230-kV Grid (Offsite Power)	Loss of Power	1×10^{-3}/hr
Motor-Operated Disconnect EDS-A	Fail to Operate	3×10^{-4}/d
Transformer ST-A	Short Circuit	1×10^{-6}/hr
Feeder Breaker 4-2A	Fail to Close	1×10^{-3}/d
Feeder Breaker 8-2A	Trip Open	1×10^{-6}/hr
Tie Breaker 11-3AS	Trip Open	1×10^{-3}/hr
Diesel Generator 1A	Fail to Start	3×10^{-2}/d
Circuit Breaker 14-3AS	Trip Open	1×10^{-3}/hr

Abnormal events in a nuclear power plant such as a loss of coolant accident results in a turbine trip. The turbine trip causes a sudden loss of electrical power generation that upsets the steady-state stability of the transmission grid. Based on information provided by the Federal Power Commission, the probability of losing offsite power because of induced power transients (turbine trip) was assessed in the Reactor Safety Study to be 1×10^{-3}/hr for any locale in the United States. This value was used in the evaluation of system reliability of the 4.16-kV ESF bus.

B. System Reliability of the 4.16-kV ESF Bus

The reliability block diagram (RBD) for the 4.16-kV ESF bus, 3AS or 3BS, is shown in Figure 7. The RBD is drawn for the major components that operate normally to provide sufficient power supply to the 4.16-kV bus for preserving the safety functions of the nuclear power plant. Based on the RBD, the system reliability based on hardware failures only is evaluated by the following equation:

$$R' = 1 - (1 - R_1R_2R_3R_4)\ (1 - R_5R_6R_7R_8) \tag{6.1}$$

$$R_{sys} = 1 - (1 - R'R_9R_{10})\ (1 - R_{11}R_{12}) \tag{6.2}$$

The estimates for the reliability (R_i) of each component to perform its design function on a single demand within a one-hour duration of the postulated accident were obtained from the associated failure data as shown on Table 4.

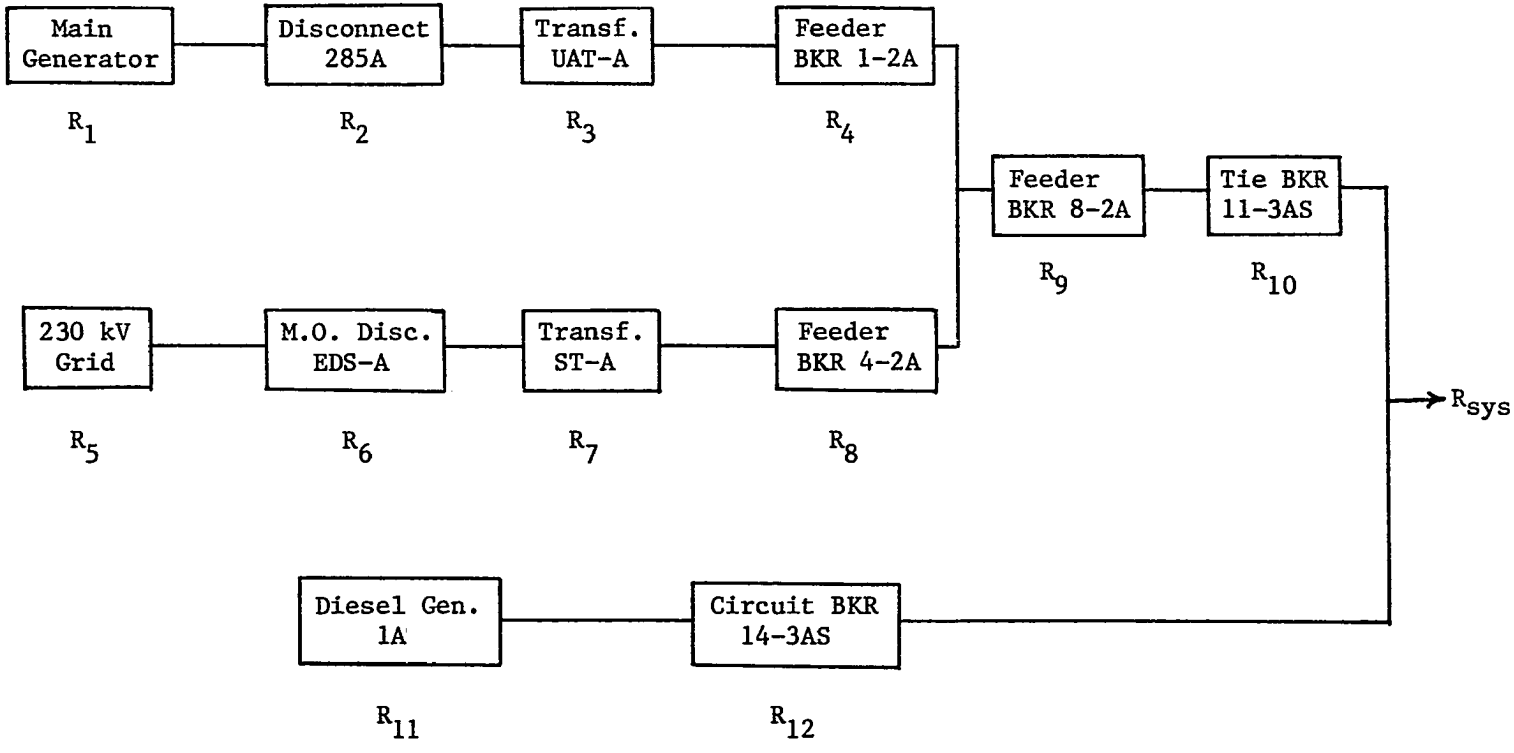


Figure 7. Reliability block diagram for a 4.16-kV ESF bus

Using the numerical values obtained for the basic component failures, the computation for system reliability was performed as follows:

$$R_1R_2R_3R_4 = \exp\{-(0.001159 + 0.000001 + 0.000001 + 0.000001)\}$$
$$= 0.998839$$

$$R_5R_6R_7R_8 = \exp\{-(0.001 + 0.0003 + 0.000001 + 0.001)\}$$
$$= 0.997702$$

$$R' = 1 - (1 - 0.998839)\ (1 - 0.997702)$$
$$= 0.999997$$

$$R'R_9R_{10} = (0.999997) \times \exp\{-(0.000001 + 0.001)\}$$
$$= 0.998997$$

$$R_{11}R_{12} = \exp\{-(0.03 + 0.001)\}$$
$$= 0.969476$$

$$R_{sys} = 1 - (1 - 0.998997)\ (1 - 0.969476)$$
$$= 0.999969$$

System unavailability, $q = 3.1 \times 10^{-5}$

System failure rate, $\lambda_s = 3.1 \times 10^{-5}$/hr

C. Fault Tree Analysis

The reliability analysis for a system must be accompanied by the identification of causal relationships between hardware, human and

environmental events. A fault tree is a graphical representation of the causal relationships obtained when a system hazard is traced backward to search for its possible causes. The probability of loss of electric power to the ESF systems during a LOCA can be evaluated by means of a Fault Tree Analysis (FTA).

The undesired event subjected to analysis in this study is the loss of electric power to the 4.16-kV ESF bus (3AS or 3BS). This event is defined as "insufficient power on bus 3AS" and is the top event of the simplified fault tree for the 4.16-kV electrical distribution system. Since this system is fully redundant, the total loss of electric power to and from the 4.16-kV electrical distribution system can only be caused by two simultaneous bus failures: one in Train A and the other in Train B. These failures are caused by failures of components or events that are essentially identical in each train. Hence, the fault analysis considered in this study is confined to the determination of the availability (or reliability) of either 4.16-kV ESF bus (3AS or 3BS) to perform its design function.

1. Initial assumptions

The construction and probabilistic evaluation of the 4.16-kV ESF bus system fault tree and the subtrees is based on the following categories of assumptions: a) general assumptions, b) human interaction and c) hardware assumptions.

a) General assumptions

i) The emergency buses (3AS and 3BS) are available during normal plant operation.

ii) Those events that appear in single or double cut sets are included in the fault trees of the individual buses asso-

ciated with the 4.16-kV ESF bus system. Nonsafety buses and loads that are isolated from the 4.16-kV ESF bus by two or more circuit breakers are not considered potential fault sources.

b) Human interaction

i) There is no credit for operator action that compensates for a failure during the first hour following a LOSP transient. This is about the time required to uncover the reactor core upon loss of electric power coincident with a loss of coolant accident. For most of this period, the operator is normally not permitted to act independently or to leave the control room.

c) Hardware assumptions

i) Distribution faults in the HV switchyard are short circuits on the buses that result from improper operation of the various circuit breakers.

ii) The batteries provide sufficient dc control power to the ESF equipment during the critical time period.

2. Description of the fault tree

The events in the fault tree are represented by a systematic coding scheme. Figure 8 shows the coding scheme, which identifies the events by system, component type, component identification and failure mode. The fault event codes used to identify the various basic events are provided in Table 5.

The simplified fault tree for the 4.16-kV ESF bus is shown in Figure 9. The three events that cause insufficient power on a 4.16-kV ESF bus can be described as follows:

a) Short circuit on bus This event includes all short circuits on the bus structure that cause the bus voltage to drop below an acceptable level.

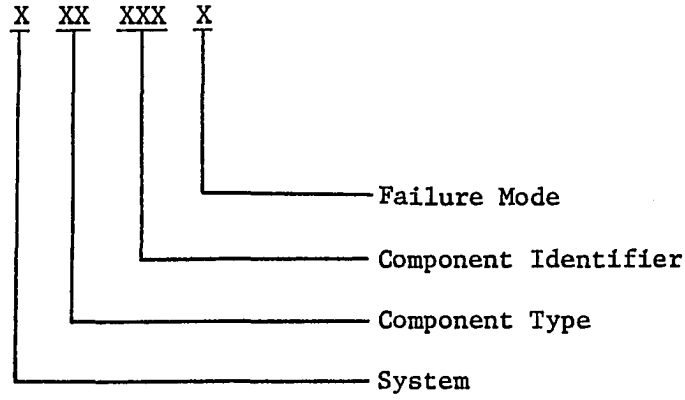


Figure 8. Coding scheme for fault event

Table 5. Fault event codes

Code	System	Code	Component	Code	Failure Mode
E	Electric	BY	Battery	A	Fail to Start
		BS	Bus	B	Open Circuit
		CB	Circuit Breaker	C	Fail to Close
		DS	Disconnect	D	Fail to Open
		DG	Diesel Generator	F	Loss of Function
		FB	Feeder Breaker	L	Loss of Power
		GE	Main Generator	O	Open
		TR	Transformer	Q	Short Circuit
		00	Event	X	Operator Error
		SY	Switchyard		

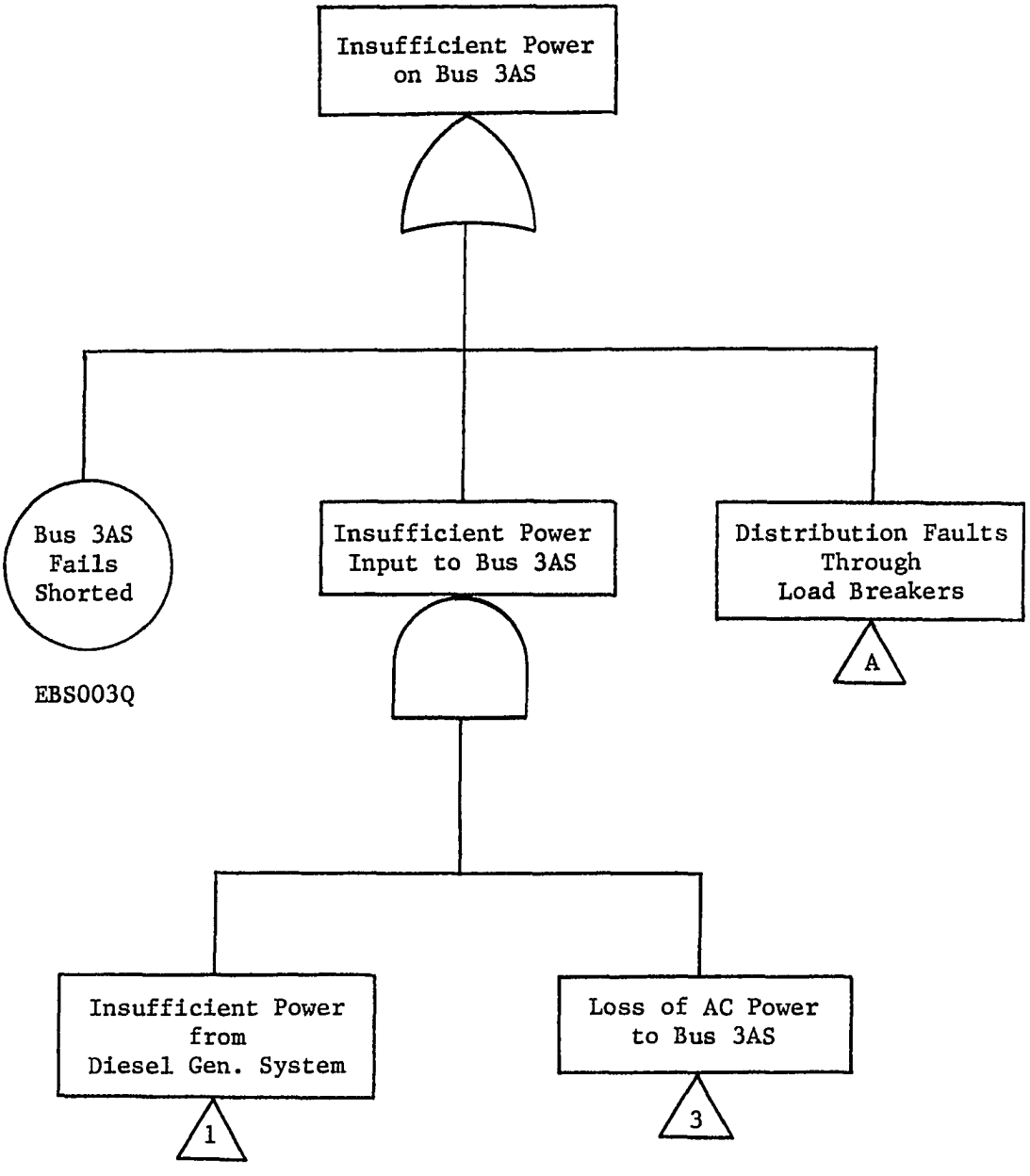


Figure 9. Simplified fault tree for a 4.16-kV ESF bus

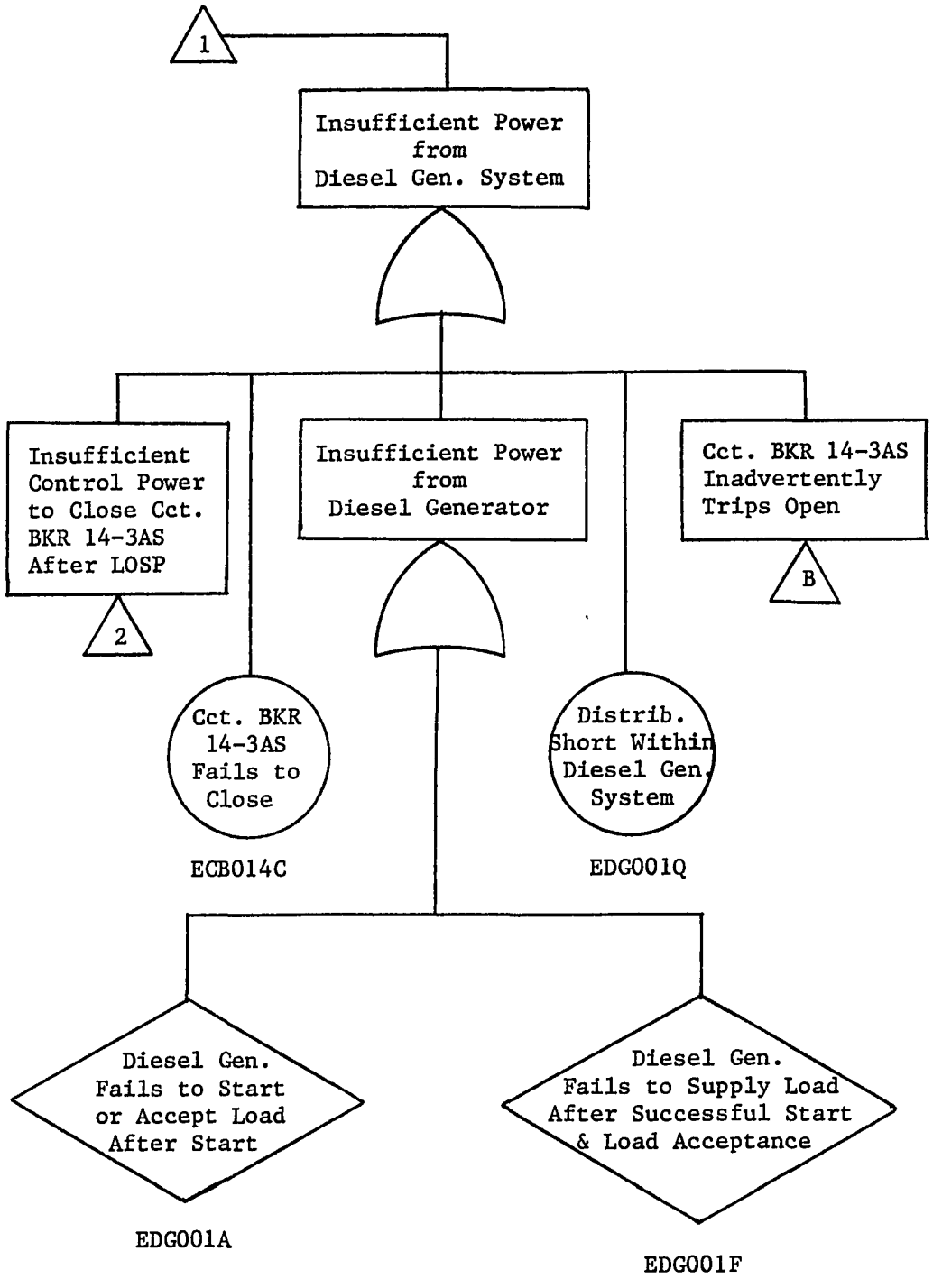


Figure 9. (Continued)

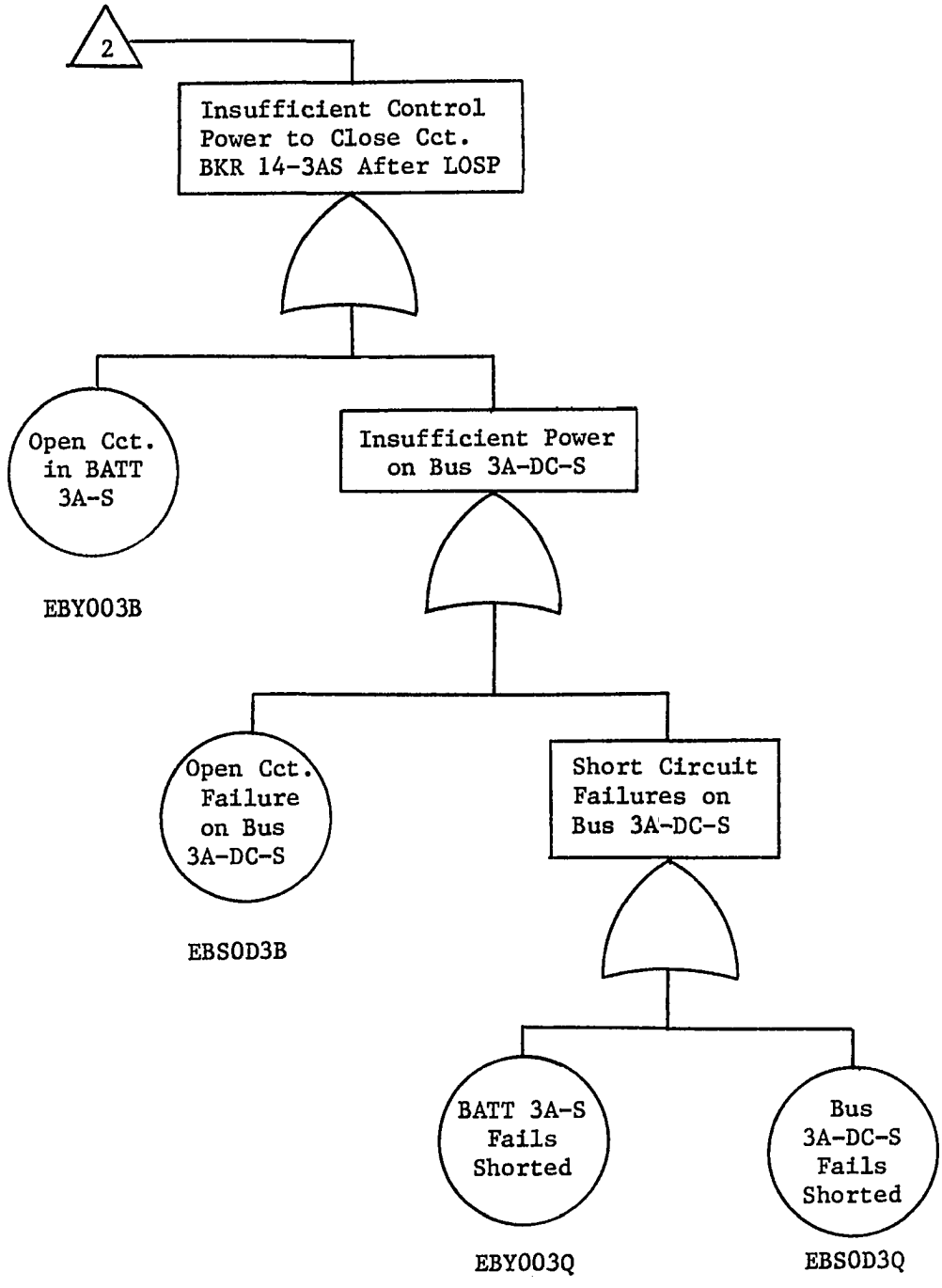


Figure 9. (Continued)

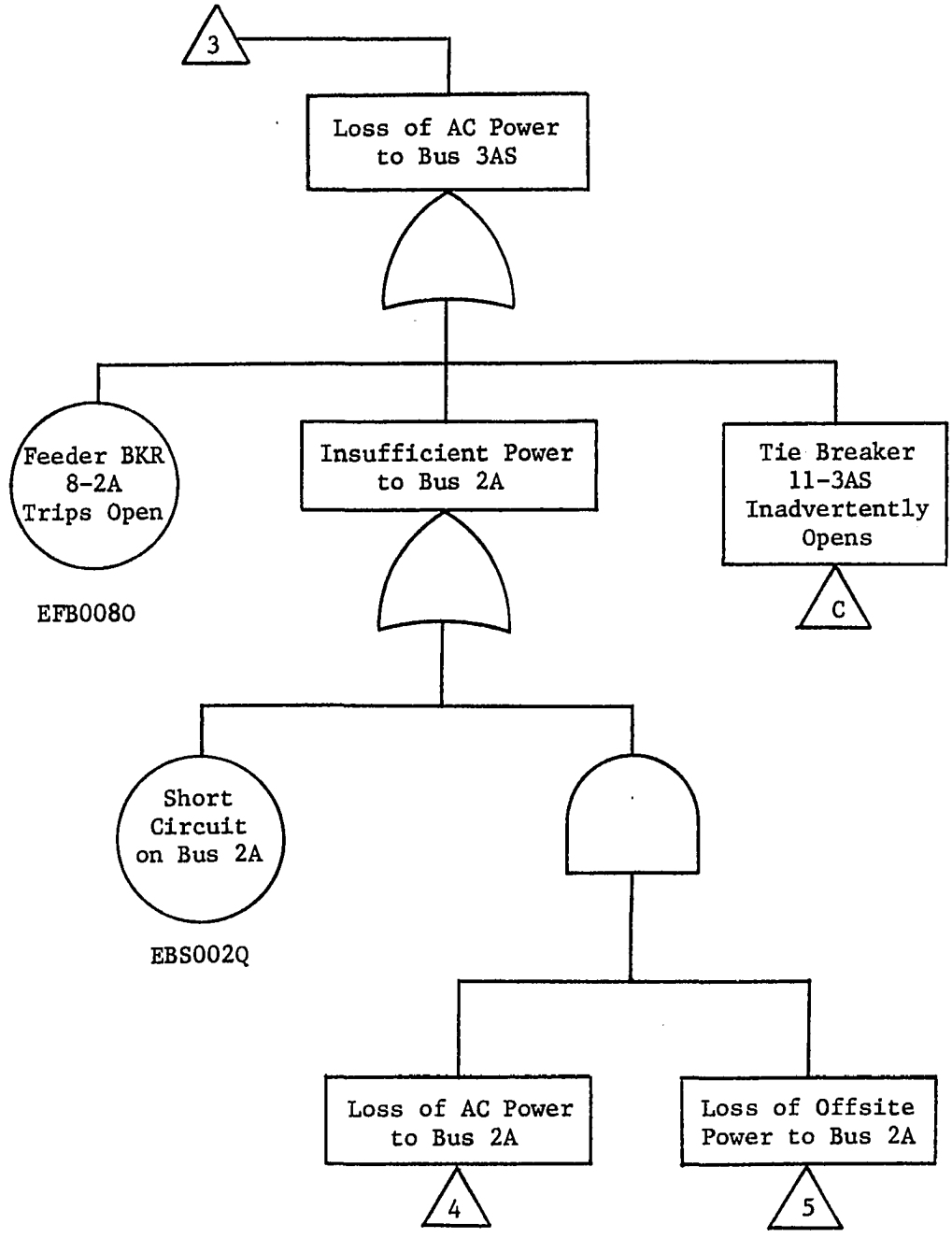


Figure 9. (Continued)

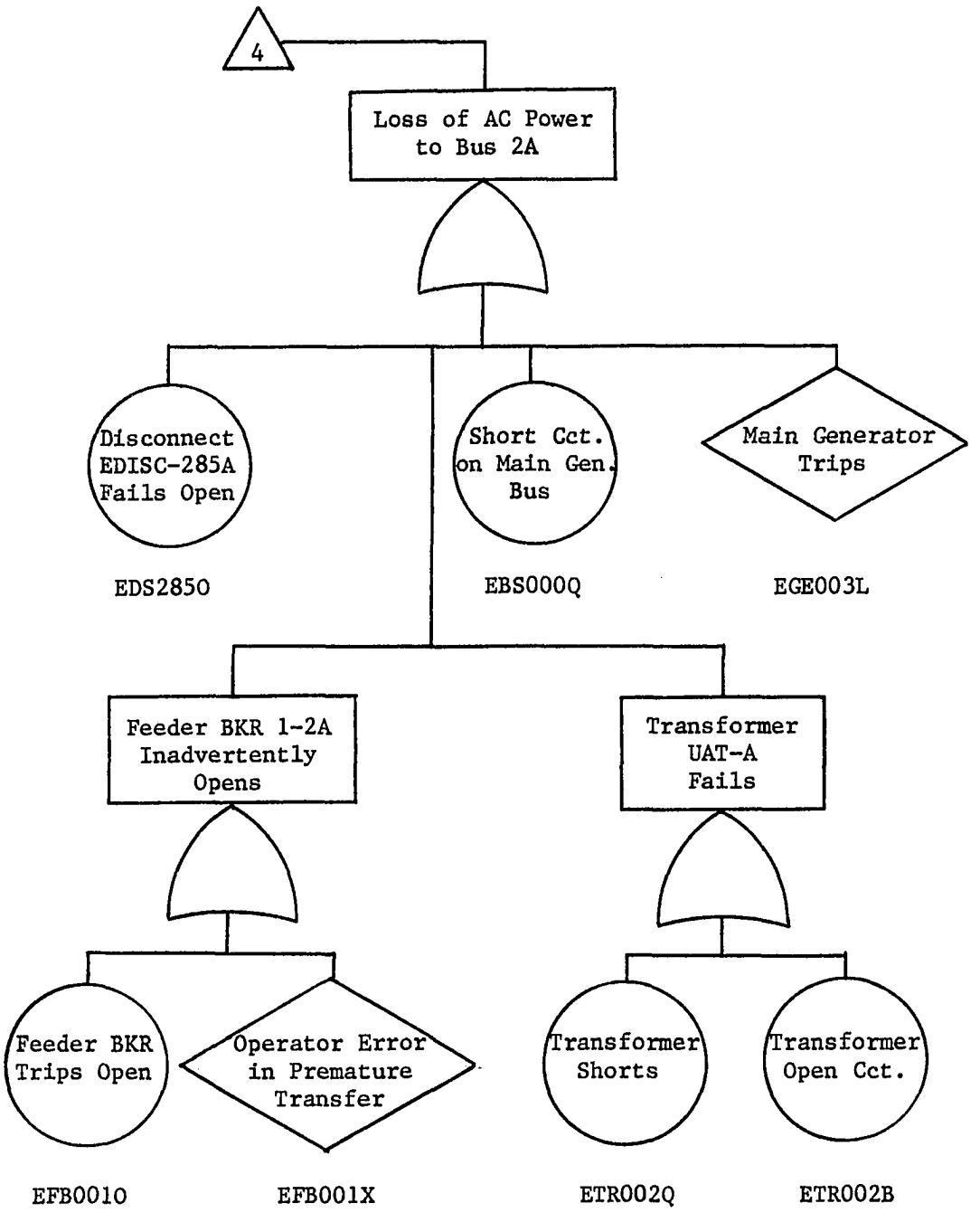


Figure 9. (Continued)

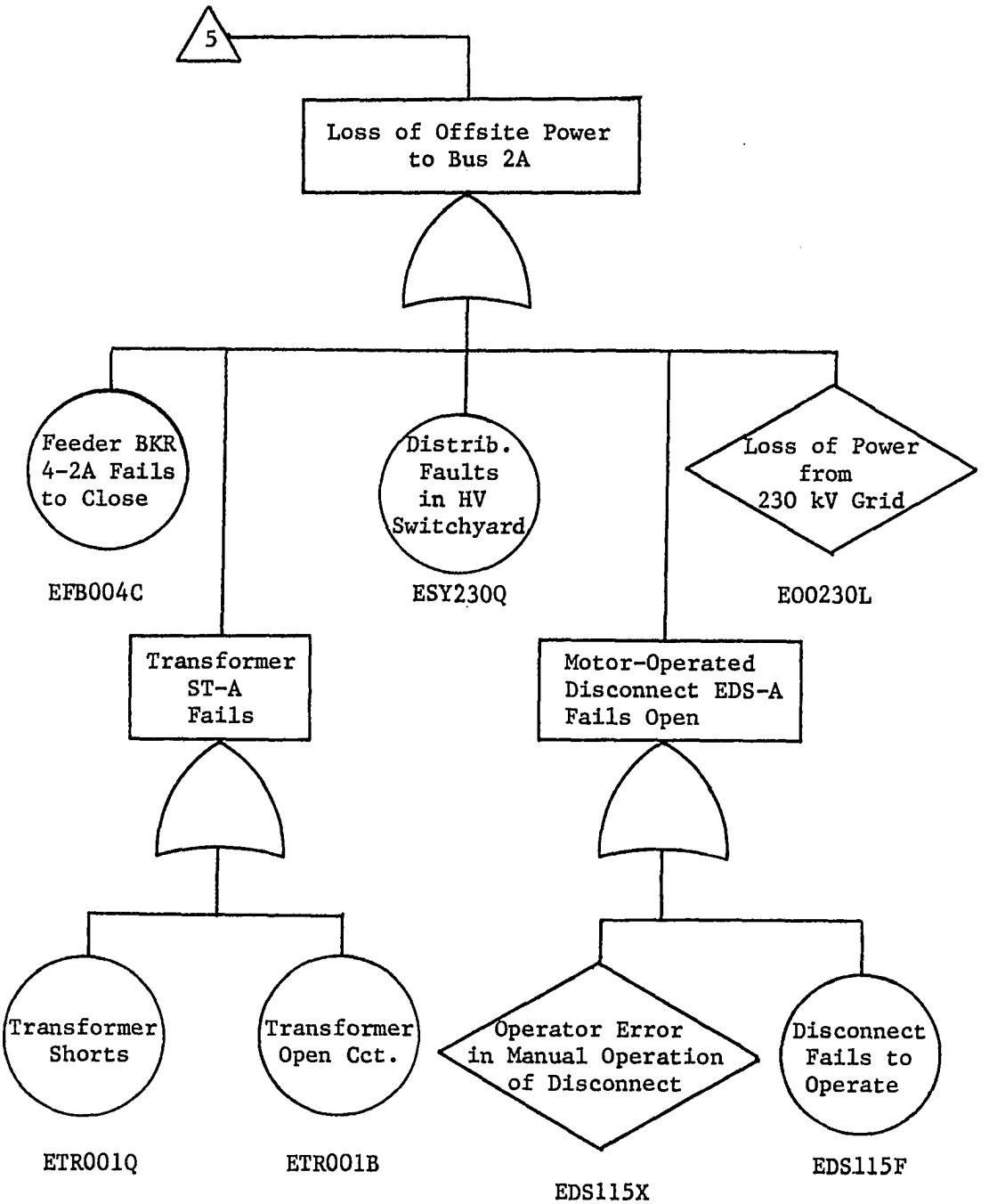


Figure 9. (Continued)

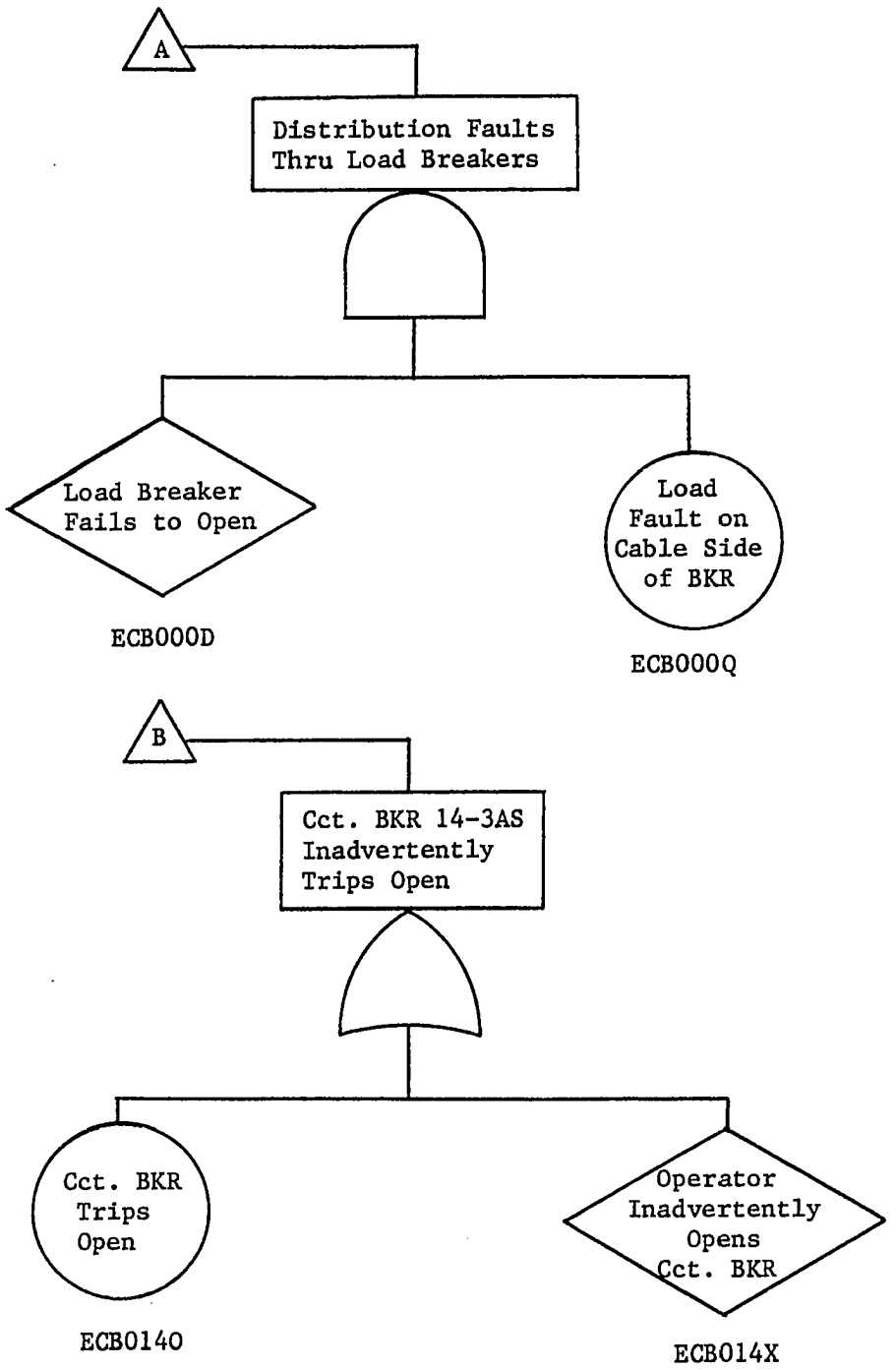


Figure 9. (Continued)

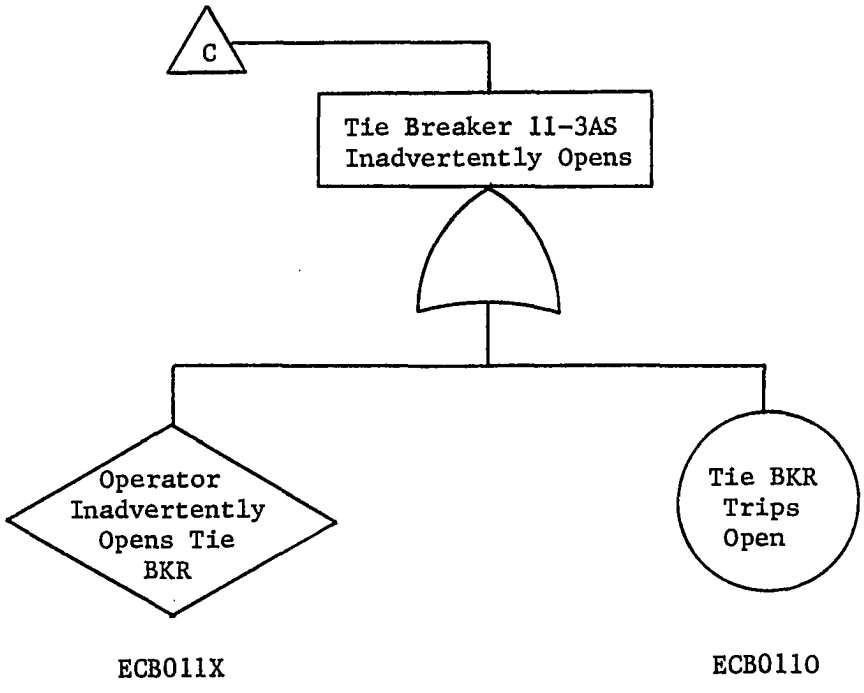


Figure 9. (Continued)

b) Insufficient power input to bus This event represents the loss of power at the bus due to external failures. Inadequate power supply to this bus can be caused by total loss of available ac power and failure of the emergency diesel generator.

c) Distribution faults through load breakers This event represents a double fault, viz., a short on any feeder cable from the bus and failure of the load breaker to open.

Insufficient power from the diesel generator system to the 4.16-kV ESF bus is primarily due to diesel generator failure to start or operate after a successful start and load acceptance. Other events that can contribute to insufficient power supply from the diesel generator system involve the output circuit breaker (14-3AS) as well as distribution shorts within the system itself. The output circuit breaker can trip open or fail to close, especially when there is insufficient control power after a LOSP transient. Inadequate control power can result from failures on the dc power system. These failures can arise from short circuits on the dc bus and its associated battery.

The total loss of available ac power can be caused by the loss of normal ac power to the connecting bus (2A) coincident with loss of offsite power. Loss of normal ac power is primarily due to a forced outage, i.e., the main generator trips as a result of an abnormal condition. Other events that can contribute to the loss of normal ac power to bus 2A are the opening of the normally closed disconnect (EDISC-285A) to the unit auxiliary transformer, a short circuit on the main generator bus, inad-

vertent opening of the feeder breaker 1-2A and failures on the unit auxiliary transformer.

The loss of offsite power to bus 2A is primarily due to loss of power from the 230-kV transmission grid caused by power instabilities or external events such as lightning, hurricanes, etc. Other events that may inhibit available offsite power to bus 2A are distribution faults in the HV switchyard, the opening of the motor-operated disconnect EDS-A, failures on the startup transformer and failure of the associated feeder breaker 4-2A to close properly on demand.

Because of equipment diversity and physical separation, the 4.16-kV electrical distribution system is not susceptible to common cause failures. No single event such as calibration errors, instrument drifts, relay settings, fire or electrical transients due to abnormal plant conditions could incapacitate the 4.16-kV electrical system. However, the offsite power source and the onsite power source can be vulnerable to common cause failures. Based on the common cause failure evaluations, the probability of losing offsite power had been estimated to be $1x10^{-3}$ [1]. Some common cause failures that could result in the unavailability of the onsite power source, i.e., the emergency diesel generator, are abnormal weather, contamination of the air-start system, dirty fuel oil, lack of lubrication, fouling of diesel generator cooling heat exchangers and dirty relay contacts.

3. Quantitative analysis

The basic events identified in the fault tree and their associated probabilities facilitate the calculation of the probability of the top

event using the Boolean algebraic process. The point estimates for the failure rates and demand failure probabilities of the various components in the system were calculated from actual operating data or obtained from industrial sources [1, 26, 27]. Table 6 shows the operating experience data for the diesel generator events identified in the system fault tree. These data provided the basis for estimating the failure probabilities associated with the diesel generators for weekly and monthly testing intervals. The basic events describing the failure modes of the various components and their associated probabilities are provided in Table 7.

Table 6. Operating experience data of Cooper-Bessemer diesel generator (4-MW rating) in commercial nuclear power plants from 1 January 1976 to 31 December 1978

Event	Number of Failures
Failure to Start	7
Failure to Continue Operating After Successful Start and Load Acceptance	12
Total Number of Demands or Number of Operating Hours = 468 (Weekly Testing)	
= 108 (Monthly Testing)	

The top event in the system fault tree is "insufficient power on bus 3AS." This event is the OR combination of bus short circuit (EBS003Q), insufficient power input to the bus 3AS and distribution faults through the load breakers. The intermediate event, "insufficient power input to

Table 7. Failure rates (λ_0) and demand failure probabilities (Q_d) for the basic events in the fault tree

Basic Event	Component	Failure Mode	Computational Median
E00230L[a]	230-kV Grid	Loss of Power	$1x10^{-3}$/hr
EDS115F[a]	Motor-Operated Disconnect EDS-A	Fail to Operate	$3x10^{-4}$/d
EDS115X[b]	Motor-Operated Disconnect EDS-A	Operator Error During Manual Operation	$1x10^{-2}$/d
ETR001B[a]	Transformer ST-A	Open Circuit	$1x10^{-6}$/hr
ETR001Q[a]	Transformer ST-A	Short Circuit	$1x10^{-6}$/hr
ESY230Q[a]	HV Switchyard	Short Circuit	$3x10^{-9}$/hr
EFB004C[a]	Feeder Breaker 4-2A	Fail to Close	$1x10^{-3}$/d
EGE003L[c]	Main Generator	Trip Out	$1.159x10^{-3}$/hr
ETR002B[a]	Transformer UAT-A	Open Circuit	$1x10^{-6}$/hr
ETR002Q[a]	Transformer UAT-A	Short Circuit	$1x10^{-6}$/hr
EFB0010[a]	Feeder Breaker 1-2A	Trip Open	$1x10^{-6}$/hr
EFB001X[b]	Feeder Breaker 1-2A	Operator Error in Premature Transfer	$1x10^{-2}$/d
EDS2850[a]	Disconnect 285A	Fail Open	$1x10^{-6}$/hr
EBS000Q[a]	Main Generator Bus	Short Circuit	$3x10^{-7}$/hr
EBS002Q[a]	Bus 2A	Short Circuit	$2x10^{-7}$/hr

[a] Appendix III, Reactor Safety Study (WASH-1400).

[b] Information in March 10, 1980 letter from D. Ross (Nuclear Regulatory Commission) to all pending Operating License Applicants of Westinghouse and Combustion Engineering NSSS designs.

[c] Estimate obtained from outage data as shown in Appendix.

Table 7. (Continued)

Basic Event	Component	Failure Mode	Computational Median
EDG001A	Diesel Generator 1A	Fail to Start	1.5×10^{-2}/d[d] 6.5×10^{-2}/d[e]
EDG001F	Diesel Generator 1A	Fail to Continue Operating After Successful Start	2.6×10^{-2}/hr[d] 1.1×10^{-1}/hr[e]
EBS0D3B[a]	Bus 3A-DC-S	Open Circuit	1×10^{-6}/hr
EBS0D3Q[a]	Bus 3A-DC-S	Short Circuit	2×10^{-7}/hr
EBY003B[a]	Battery 3A-S	Open Circuit	1×10^{-6}/hr
EBY003Q[a]	Battery 3A-S	Short Circuit	3×10^{-6}/hr
EDG001Q[a]	Diesel Generator 1A	Short Circuit	1×10^{-8}/hr
ECB014C[a]	Circuit Breaker 14-3AS	Fail to Close	1×10^{-3}/d
ECB0140[a]	Circuit Breaker 14-3AS	Trip Open	1×10^{-3}/hr
ECB014X[b]	Circuit Breaker 14-3AS	Operator Error in Commission or Omission	1×10^{-2}/d
ECB0110[a]	Tie Breaker 11-3AS	Trip Open	1×10^{-3}/hr
ECB011X[b]	Tie Breaker 11-3AS	Operator Error in Commission or Omission	1×10^{-2}/d
EFB0080[a]	Feeder Breaker 8-2A	Trip Open	1×10^{-6}/hr
ECB000D[a]	Load Breaker on Bus 3AS	Fail to Open	1×10^{-3}/d
ECB000Q[a]	Load Breaker on Bus 3AS	Short Circuit	1×10^{-7}/hr
EBS003Q[a]	Bus 3AS	Short Circuit	2×10^{-7}/hr

[d]Estimates from operating experience data of diesel generators as shown in Table 6 for a weekly testing interval.

[e]Estimates from operating experience data of diesel generators as shown in Table 6 for a monthly testing interval.

bus 3AS," is the combination of "insufficient power from the diesel generator system" AND "loss of ac power to bus 3AS." Distribution faults through the load breakers is the combination of breaker failure to open (ECB000D) AND load faults on the cable side of a breaker (ECB000Q).

The event "insufficient power from the diesel generator system" is the OR combination of four primary fault events and two intermediate events. The primary events are diesel generator failure to start (EDG001A) or operate after a successful start (EDG001F), circuit breaker 14-3AS failure to close (ECB014C) and distribution shorts within the diesel generator system (EDG001Q). The intermediate events are "circuit breaker 14-3AS inadvertently trips open" and "insufficient control power to close circuit breaker 14-3AS after LOSP." Circuit breaker 14-3AS inadvertently trips open from the combination of operator error (ECB014X) OR failure by itself (ECB0140). Insufficient control power to close circuit breaker 14-3AS is the OR combination of failures on the dc power system such as short or open circuits on the dc bus (EBS0D3Q, EBS0D3B) and battery failures (EBY003Q, EBY003B).

The event "loss of ac power to bus 3AS" is the OR combination of a basic event and two intermediate events. The basic event is the feeder breaker 8-2A trips open (EFB0080). The intermediate events are "insufficient power to bus 2A" and "tie breaker 11-3AS inadvertently opens." Insufficient power to bus 2A can result from a bus short circuit (EBS002Q) OR the logic combination of "loss of ac power to bus 2A" AND "loss of offsite power to bus 2A." The tie breaker 11-3AS inadvertently opens

from the combination of operator error (ECB011X) OR failure by itself (ECB0110).

Loss of ac power to bus 2A is the OR combination of three basic events and two intermediate events. The basic events are the opening of disconnect EDISC-285A (EDS2850), short circuit on main generator bus (EBS000Q) and main generator failure or tripout (EGE003L). The intermediate events are "feeder breaker 1-2A inadvertently opens" and " transformer UAT-A fails." Feeder breaker 1-2A trips open from the combination of operator error in premature transfer (EFB001X) OR failure by itself (EFB0010). The failures in the unit auxiliary transformer are shorts (ETR002Q) OR open circuit failure (ETR002B).

Loss of offsite power to bus 2A is also the OR combination of three basic events and two intermediate events. The basic events are the loss of power from the 230-kV grid (E00230L), distribution faults in the HV switchyard (ESY230Q) and feeder breaker 4-2A failure to close (EFB004C). The intermediate events are "transformer ST-A fails" and "motor-operated disconnect EDS-A fails open." The failures in the startup transformer are shorts (ETR001Q) OR open circuit failure (ETR001B). The motor-operated disconnect EDS-A fails open from the combination of operator error during the manual operation of disconnect (EDS115X) OR failure to operate (EDS115F).

The overall system unavailability was evaluated for a single demand of the various components to function during a one-hour interval of the postulated accident. The probability of the event "insufficient power on bus 3AS" was computed based on the loss of electric power to the individ-

ual buses connected to it. This event was evaluated for two cases of testing interval for the emergency diesel generator: i) weekly, and ii) monthly. The occurrence probability of the top event was quantified by the Boolean process where the AND gate event is a multiplicative combination and the OR gate is an additive combination of the input events. The summary of the quantification process for the fault tree analysis of the emergency power system is shown in Table 8.

Table 8. Quantification results of the fault tree

Event Description	Unavailability (q)	
	Case I	Case II
Loss of Offsite Power to Bus 2A	1.23×10^{-2}	1.23×10^{-2}
Loss of ac Power to Bus 2A	1.12×10^{-2}	1.12×10^{-2}
Loss of ac Power to Bus 3AS	1.11×10^{-2}	1.11×10^{-2}
Insufficient Control Power to Close Circuit Breaker 14-3AS After LOSP	5.2×10^{-6}	5.2×10^{-6}
Insufficient Power from Diesel Generator System	5.3×10^{-2}	1.87×10^{-1}
Insufficient Power on Bus 3AS	5.88×10^{-4}	2.08×10^{-3}

D. Conclusions

Using data primarily from Appendix III of the Reactor Safety Study, the reliability of the 4.16-kV ESF bus based on the RBD model for hardware failures only was evaluated to be 0.999969. This provides the probability of 4.16-kV bus unavailability per demand as 3.1×10^{-5}. The summary for the quantification results of the fault tree shows that the estimated probability of 4.16-kV bus unavailability per demand are 5.88×10^{-4} and 2.08×10^{-3} for the weekly and monthly testing of diesel generators.

The fault tree analysis shows that loss of offsite power (LOSP) is an important contributor to the overall unavailability of the 4.16-kV ESF bus. Loss of offsite power is an anticipated transient which could lead to power-coolant (or thermal-hydraulic) imbalances in a nuclear power plant. The automatic plant responses to the LOSP transient can be investigated by an event tree. The relevant operator actions to mitigate the effects of this initiator can be effectively analyzed by the operator action event tree (OAET). The OAET can identify the risk significant sequences that may evolve from this transient.

VII. THE OPERATOR ACTION EVENT TREE

The operator action event tree (OAET) is constructed to address the role of the reactor operator responding to the abnormal conditions initiated by a transient event. The OAET presents a logical display of the significant aspects of this role throughout the incident. This permits the qualitative analysis of the event sequence and of the relevant operator action to preclude or mitigate the effects of the transient-initiated conditions.

The initiating event in the OAET is defined as the loss of offsite power (LOSP) to the nuclear plant after a main generator outage. This results in loss of available ac power for the reactor coolant pumps, condensate pumps, circulating water pumps, and pressurizer pressure and level control systems. Under these circumstances, the nuclear plant would experience simultaneous losses of load, of feedwater flow and of forced reactor coolant flow.

When normal ac power is lost to the nuclear plant, all four reactor coolant pumps "coast down" and a reactor trip occurs due to low reactor coolant flow. The turbine stop valves close and an automatic turbine trip follows. The main feedwater flow to both steam generators decreases rapidly. The pressure increases in the reactor coolant system (RCS) and steam generator, but pressure rise is limited by the primary (pressurizer) and steam generator safety valves. On loss of normal ac power, the emergency diesel generators are automatically started to provide ac power

supply to limited loads on the engineered safety feature buses (4.16-kV buses 3AS and 3BS).

After a reactor trip, the decay heat must be dissipated by the main steam system to the environment. In the absence of forced reactor coolant flow, convective heat transfer is supported by natural circulation of reactor coolant flow. Initially, the residual water inventory in the steam generators provides a heat sink and the resultant steam is released to the atmosphere by the steam generator safety valves. Emergency feedwater supply is automatically initiated when low steam generator water level is reached. Plant cooldown is controlled by the atmospheric steam dump valves if normal power is not restored within thirty minutes. Operator action is delayed until thirty minutes after the event.

After the initiation of the LOSP event, the availability of the diesel generator to supply emergency ac power is critical throughout the sequence of events. Emergency ac power is required to operate the motor-driven emergency feedwater pumps, the safety injection pumps, the component cooling water pumps and the containment spray pumps. Therefore, the dominant risk sequences in the event involve the unavailability of the diesel generators.

While removing decay heat and thereafter, adequate reactor coolant inventory must be maintained. Reactor coolant inventory is replenished by actuation of the safety injection pumps and the charging pumps. These pumps are aligned to take suction from the refueling water storage pool (RWSP) to provide the required makeup supply of borated water.

The OAET constructed for the LOSP initiator is shown in Figure 10. The basic states to which the nuclear plant could evolve are identified. The required operator responses relevant to the indicated states of the event tree are addressed.

STATE LOSP-1:

State 1 represents the automatic plant responses to the LOSP event and successful decay heat removal through secondary steam relief. The important automatic responses are reactor trip (scram), reactor coolant pump trip, main feedwater pump trip, circulating water pump trip and starting of the diesel generators. These responses result in a reactor condition at decay heat power level with reduced heat removal capability through the steam generators by main feedwater cooling. The reactor coolant flow is "coasting down." The reactor coolant system (RCS) experiences depressurization as the average reactor coolant temperature ($T_{avg.}$) decreases after a brief rapid increase. The steam flow is isolated by the closure of the turbine stop valves and the secondary steam pressure reaches the setpoint of the atmospheric dump valves (ADV).

Required Operator Action:

The operator is restricted to the diagnosis of the LOSP initiator and verification of the automatic responses. The operator then directs attention to establishing heat removal through the steam generators and maintaining adequate coolant inventory. If automatic steam relief is not achieved through the ADV or steam generator safety relief valves, the operator must manually produce secondary steam relief by opening the two ADVs.

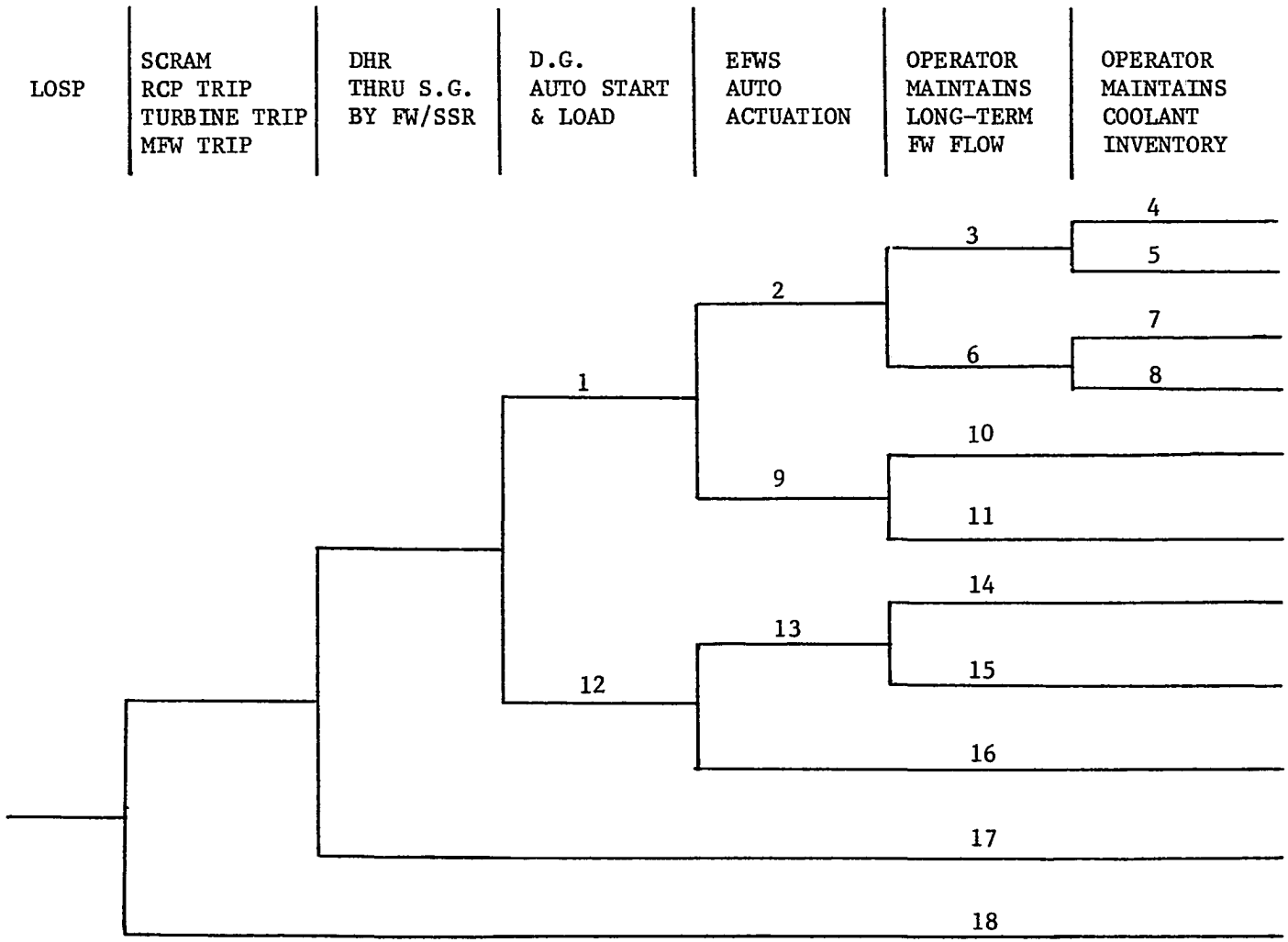


Figure 10. Operator action event tree for a LOSP initiator

STATE LOSP-2:

State 2 describes the situation after the successful automatic delivery of emergency feedwater to the steam generator. The automatic plant response to the LOSP initiator has continued success. An adequate heat sink is provided for dissipation of decay heat in the primary system.

Required Operator Action:

The operator has to recognize successful automatic emergency feedwater system (EFWS) operation and maintain long-term EFW delivery by throttling flow and aligning the EFW pumps to the auxiliary component cooling water system (ACCWS) for emergency backup source of water if the condensate storage pool (CSP) becomes depleted. The motor-driven and turbine-driven EFW pumps start upon receipt of the emergency feedwater actuation signal (EFAS) and deliver rated flow to the steam generator. The operator must throttle the EFW flow in about one hour to prevent "steam generator overfill" on the secondary side. Otherwise, the CSP will also be depleted in about 2.5 to 3 hours. The operator then would be required to align the system to the ACCWS for a backup source of emergency feedwater.

STATE LOSP-3:

State 3 shows adequate feedwater flow to the steam generators is maintained after controlled flow is achieved and the EFWS is aligned to a backup source of feedwater. Heat removal from the primary system through emergency feedwater cooling in the steam generator is successful.

Required Operator Action:

The operator has to verify stable feedwater delivery and then focus attention on maintaining coolant inventory.

STATE LOSP-4:

State 4 represents the plant condition where the diesel generators started automatically and continued operating with the long-term heat removal through the steam generators successfully maintained after the LOSP event. The primary system boundary and steam generator tube integrity remains intact.

Required Operator Action:

As a result of successful plant response, the only operator concern is to ensure that adequate coolant inventory is maintained throughout the plant cooldown. This requires appropriate charging flow to compensate for any mass loss through the pressurizer relief valve and level reductions due to fluid cooldown.

STATE LOSP-5:

State 5 depicts the situation where the operator is able to maintain long-term feedwater flow to the steam generator, but the RCS inventory is depleting through (i) a steam generator tube rupture, or (ii) a stuck-open pressurizer relief valve. In the steam generator tube rupture incident, slightly radioactive coolant flows into the secondary system and out of the containment. The stuck-open pressurizer relief valve constitutes a small break loss-of-coolant accident (LOCA).

Required Operator Action:

For the steam generator tube rupture incident, the operator has to identify and isolate the affected steam generator. He has to adjust

safety injection (SI) flow into the RCS to compensate for flow out through the ruptured tube. Then, the primary system is to be depressurized using the pressurizer relief valves and by blow-down of the intact steam generator. This pressure reduction decreases the primary-to-secondary flow through the rupture. Once the leak flow is stopped by the equalization of pressures in the RCS and the affected steam generator, normal plant cooldown can be commenced.

In the case of a stuck-open pressurizer relief valve, the operator has to close the valve and ensure adequate SI flow into the RCS to compensate for mass spill out of the stuck-open valve.

STATE LOSP-6:

State 6 represents the situation where long-term feedwater flow could not be maintained after the successful automatic EFWS initiation. This could be due to failure of pumps to continue running, or operator failure to throttle feedwater flow or align backup water to replenish the CSP. This state also assumes the inability to use the condensate pumps to deliver feedwater because offsite power is unavailable. Hence, the steam generator could not be used as a long-term heat sink.

Required Operator Action:

The operator begins the "feed and bleed" operation as an alternate means of heat removal. This operation requires that energy is to be released through the pressurizer relief valve and using high pressure safety injection (HPSI) pumps to maintain RCS inventory. The operator must manually depressurize ("bleed") the primary system by keeping the pressurizer relief valves open and maintain controlled HPSI flow ("feed")

to avoid core damage due to uncovery. Cold shutdown can then be safely achieved in a timely fashion.

STATE LOSP-7:

This state represents the plant condition following the successful "feed and bleed" operation to accomplish the heat removal from the RCS and maintenance of its inventory.

Required Operation Action:

The only operator concern is to monitor the progress of a safe cold shutdown.

STATE LOSP-8:

State 8 represents the plant state where feedwater delivery could not be maintained and the RCS inventory is depleting through either tube ruptures in a steam generator due to dryout or a stuck-open pressurized relief valve.

Required Operator Action:

The operator must take actions to actuate the safety injection system to inject borated water into the RCS for adequate heat removal and inventory maintenance to prevent cladding failures upon core uncovery. The plant cooldown process must be closely monitored for any contingencies.

STATE LOSP-9:

This state describes the plant condition when the EFWS fails to automatically supply feedwater to the steam generator after a successful start of the emergency diesel generators. The turbine-driven pump and both motor-driven feedwater pumps have failed to deliver sufficient flow to the steam generators due to either valving errors in the feedwater lines or pump failures.

Required Operator Action:

On recognition of the EFWS failure, the operator should attempt to achieve adequate feedwater flow by starting one of the EFW pumps or by blowing down one or more steam generators. If the operator can actuate the turbine-driven pump and a single motor-driven EFW pump within ninety minutes after the LOSP event, damage to the core can be prevented. If the operator ascertains that EFW flow is unavailable, he should implement safety injection of subcooled water into the primary system. SI flow can be enhanced by depressurization in the RCS via steam generator blow-down.

STATE LOSP-10:

At this state, the operator has achieved delayed feedwater flow after initial failure to automatically provide EFW flow. The turbine-driven EFW pump or the motor-driven pumps have been restored to service. The maintenance of long-term feedwater flow provides an adequate heat sink for primary system decay heat removal.

Required Operator Action:

Same as state 3.

STATE LOSP-11:

This state represents the plant condition where the operator fails to achieve delayed feedwater flow following the failure of the EFWS to automatically actuate. There is no stable long-term heat removal path through the steam generator.

Required Operator Action:

The operator must begin the "feed and bleed" operation for adequate cooling of the RCS.

STATE LOSP-12:

At state 12, the emergency diesel generator failed to start automatically after the LOSP event. The diesel generator failure results in the unavailability of the motor-driven EFW pumps, the safety injection and charging pumps, and component cooling water to the reactor coolant pump seals. Without the motor-driven EFW pumps, heat removal through the steam generator depends on the successful actuation of the turbine-driven pump. Without the safety injection or charging pumps, fluid loss from the RCS cannot be replenished. Without component cooling water, leakage past the reactor coolant pump seals can occur.

Required Operator Action:

After recognizing the successful automatic responses to the LOSP event (e.g., scram, RCP trip, etc.) and the failure of diesel generators to start and load, the operator has to ensure actuation of the turbine-driven EFW pump and attempt to restore the diesel generators to operability. At this state, the station batteries become the sole source of power supply to the dc buses and the ac vital instrumentation buses. This power supply must be conserved since there is no emergency ac power to charge the batteries.

STATE LOSP-13:

At state 13, the turbine-driven EFW pump has actuated automatically after the LOSP event and failure of the diesel generators. This pump delivers sufficient flow to the steam generators to provide a heat sink for decay heat. This state is similar to that at state 2 except for the unavailability of the diesel generators.

Required Operator Action:

The operator should verify successful turbine-driven EFW pump flow and continue attempts to start the diesel generator. Also, he has to throttle feedwater flow to prevent overfill and help maintain long-term feedwater flow. He should decrease primary system pressure to reduce any excessive reactor coolant pump seal leakage. Sufficient reduction in primary system pressure will permit safety injection tank (SIT) discharge to compensate for large seal leakages.

STATE LOSP-14:

At state 14, the operator maintains controlled EFW flow through the turbine-driven pump. This provides a stable long-term heat sink through the steam generators.

Required Operator Action:

The operator has to verify stable heat removal through the steam generators and begin necessary actions to maintain adequate primary coolant inventory. The specific actions are to replenish mass loss through an open pressurizer relief valve and ensure adequate safety injection into the RCS to compensate for flow out through a steam generator tube rupture.

STATE LOSP-15:

At this state, the successful automatic feedwater delivery achieved at state 13 is not sustained. The capability for heat removal through the steam generators is lost.

Required Operator Action:

The operator should initiate "feed and bleed" cooling as an alternate means of decay heat removal while maintaining adequate coolant inventory.

STATE LOSP-16:

State 16 describes the failure of the EFWS to provide adequate flow to the steam generators after the LOSP event compounded by failure of the diesel generators to start. The decay heat load is not removed from the primary system through the steam generators. Since the diesel generators may be unavailable, HPSI into the primary system could not be initiated.

Required Operator Action:

The operator has to secure a source of ac power by attempting to start a diesel generator within 4500 seconds or restore off-site power. Core uncovery is predicted to occur after this time. Once emergency ac power becomes available, the operator should establish a "feed and bleed" mode of cooling and maintain RCS inventory through charging flow.

STATE LOSP-17:

This state addresses the situation where a steam generator safety relief valve rupture occurs in coincidence with a LOSP event. After the LOSP initiator and the resultant trip of the main feedwater pumps, the secondary system pressure increases and reaches the setpoint of a safety relief valve. The diesel generators are available to supply emergency ac power.

Required Operator Action:

The operator diagnoses the automatic responses to the LOSP initiator and the rupture of the safety relief valve. The relief valve rupture affects the operator intervention to ensure the stable long-term feedwater flow to the steam generators. The operator should observe the coincident low level and low pressure on the secondary side of the damaged

steam generator. Feedwater flow to this affected steam generator should be decreased to prevent sudden overcooling. Charging flow for maintaining RCS inventory has to be throttled to prevent filling up the pressurizer completely.

STATE LOSP-18:

State 18 describes the failure of the automatic plant responses to the LOSP event. Failure of reactor scram could lead to core uncovery and subsequent cladding failures in the fuel assemblies.

Required Operator Action:

The operator should restore offsite ac power, or undertake appropriate actions to start and load the diesel generators as soon as practical. The restored ac power enables forced reactor coolant flow using the reactor coolant pumps. EFW can be provided for heat removal through the steam generators. The charging pumps can be actuated to provide reactor coolant makeup to maintain RCS inventory. These actions should mitigate the consequences of the event.

A. Summary

The OAET identified eighteen possible states that the nuclear power plant could evolve from the LOSP initiator. The state LOSP-1 corresponds to the "basic PWR transient response" where all safety functions are preserved. The states LOSP-2, LOSP-3 and LOSP-4 depict the plant condition where decay heat in the primary system is successfully removed through the steam generators. The states LOSP-5 and LOSP-8 describe a

scenario where RCS inventory is depleting through a steam generator tube rupture or a stuck-open pressurizer relief valve. The state LOSP-6 shows the loss of a long-term heat sink in the steam generator while state LOSP-7 represents the successful accomplishment of heat removal from the RCS by a "feed and bleed" operation.

The states LOSP-9, LOSP-10 and LOSP-11 involve the loss of main feedwater initiator coupled with failure of the emergency feedwater system. State LOSP-12 and the plant states LOSP-13, LOSP-14, LOSP-15 and LOSP-16 that evolve from it involve the loss of offsite power initiator coincident with the subsequent failure of both diesel generators. The state LOSP-17 addresses the failure of steam generator safety relief valve coincident with a LOSP transient. State LOSP-18 describes the failure of the automatic plant responses to the transient that could lead to eventual degradation of the reactor core.

VIII. CONCLUSIONS AND RECOMMENDATIONS

The application of probabilistic risk assessment methodology to the evaluation of the availability of the emergency power system (EPS) to perform its design function has been successfully demonstrated in this study. The comprehensive qualitative and quantitative assessment of system availability using a reliability block diagram (RBD) model and fault tree logic provides important conclusions about the reliability of the EPS during a loss of offsite power (LOSP) transient. The operator action event tree (OAET) analysis provides a systematic identification of thermal-hydraulic responses of the principal nuclear reactor systems to the LOSP initiator and the relevant operator actions to mitigate the effects of the abnormal conditions.

A. Conclusions

Based on the system reliability analysis, the following conclusions can be stated:

1. Using data from the Reactor Safety Study (RSS), the reliability of the 4.16-kV ESF bus based on the RBD model for hardware failures only was assessed to be 0.999969. This value translates into the probability of 4.16-kV bus unavailability per demand as 3.1×10^{-5}. The RSS assessment of insufficient power to the 4.16-kV ESF bus on a single demand yields a probability of unavailability as 4.1×10^{-5}. However, this RSS assessment in-

corporated human errors in addition to hardware faults in the quantitative analysis using fault tree logic.

2. The quantitative assessment using fault tree logic in this study shows that the estimated probabilities of 4.16-kV bus unavailability per demand are 5.88×10^{-4} and 2.08×10^{-3} for the weekly and monthly testing of diesel generators respectively. These estimates are orders of magnitude higher than the probability of unavailability assessed in the RSS. The results of the study here indicate that the weekly testing interval for diesel generator operability contributes to an increased availability of the 4.16-kV ESF bus on a single demand.
3. The quantitative analysis of the system fault tree shows that human errors in commission or omission contribute significantly to overall unavailability of the 4.16-kV bus. The predominant human errors in commission involve the operation of "system-critical" components such as the circuit breakers connecting the feeders from the various power sources to the 4.16-kV bus.
4. The fault tree analysis shows that the dominant cause of insufficient power from the diesel generator system is failure of the emergency diesel generator to continue operating after a successful start and load acceptance. The short-term operational unreliability of the diesel generator after a successful start can be attributed to dirty fuel oil filters, lack of lubrication, failed bearings and "dry starts" of the diesel generators.

These circumstances are all related to poor maintenance, which is another sort of failure, but one that was not specifically addressed in this study.

5. The availability of the dc power system to provide sufficient control power required to operate the "system-critical" circuit breaker (14-3AS) depends on the reliability of the power supplies, viz., the station batteries. Since the probability of failure of dc power supplies is very small, the availability of sufficient control power to actuate the circuit breaker after a LOSP initiator represents a very small contribution to the 4.16-kV ESF bus unavailability.
6. The availability of normal ac power to 4.16-kV ESF bus is susceptible to operator errors in the premature transfer of the circuit breaker (1-2A) connecting the feeder to the connecting bus 2A. The loss of ac power is primarily caused by the main generator outage which contributes quite significantly to overall 4.16-kV ESF bus unavailability.
7. The availability of offsite power on demand is vulnerable to operator errors during the manual operation of the motor-operated disconnect (EDS-A) which connects the switching station to the startup transformers. The loss of power from the 230-kV grid also contributes to the overall 4.16-kV ESF bus unavailability.

From the OAET analysis that identified the various plant states that evolve from the LOSP transient, the following observations can be stated:

1. The state LOSP-1 corresponds to the "basic PWR transient response" where all the safety functions are maintained by automatic actuation of the plant protection system. This state is applicable to most transient initiators except that the automatic reactor coolant pump (RCP) trip is typical for the LOSP initiator. However, the availability of the RCPs does not have a significant impact on the behavior of process variables such as pressure, temperature and fluid level in the primary and secondary systems.
2. State LOSP-12 and the plant states 13-16 that evolve from it are equivalent to the TMLB'[1] accident sequence addressed in the RSS. This sequence involves the loss of offsite power initiator coincident with the subsequent failure of both diesel generators.
3. State LOSP-1 and the plant states 9-11 that evolve from it are equivalent to the TML[1] accident sequence addressed in the RSS. This sequence involves the loss of main feedwater initiator coupled with the failure of the emergency feedwater system.
4. The plant states LOSP-5 and LOSP-8 in the OAET addresses the TMLQ[1] sequence that occurred at the TMI-2 nuclear facility. This sequence involves the loss of both main and emergency feedwater compounded by a stuck-open pressurizer valve.
5. The OAET shows that the availability of the diesel generators is significant throughout the accident progression. Emergency ac

---

[1]The notations TMLB', TML and TMLQ are nomenclature for specific PWR transient sequences identified by these names in the RSS.

power is essential for the actuation of the safeguards equipment to prevent core uncovering.

The reliability analysis of the 4.16-kV ESF bus in this study shows that the overall system unavailability is significantly higher than the RSS assessment. The updated failure probabilities for the human errors and the various hardware faults account for these less optimistic results. The significant contributors to overall system unavailability are: diesel generator operability problems, particularly those associated with longer testing intervals; and human errors during the manual actuation of "system-critical" components. The low failure probability of the dc power system does not contribute strongly to maintaining overall system availability on demand.

Since the dominant contributor to the system availability is diesel generator operability on demand, a higher level of redundancy for emergency ac power can be provided by a "swing" diesel generator. The "swing" diesel generator can be aligned to the ESF bus upon a priority demand signal that arises from operability fault of the dedicated diesel generator. A viable option for increased system availability is to replace the emergency diesel generator with a more reliable source of ac power such as the gas turbine generator. This is also a cost-effective measure because the gas turbine generator provides added generating capacity when there is no demand for emergency power supply.

The OAET analysis in this study has identified the risk-significant accident sequences, viz., TMLB', TML and TMLQ which involve failures of the diesel generator system and feedwater delivery. The analysis also

shows that the delivery of emergency feedwater to the steam generators is critically dependent on the availability of the diesel generators. The likelihood of these accident sequences can be minimized by an alternate source of emergency feedwater independent of the existing motor-driven and turbine-driven systems.

Finally, the relevant operator responses to the various plant conditions identified in the OAET provide valuable lessons in an operator training program to mitigate the consequences of transient initiators. Operator training should stress the unique role of the individual in performing the necessary actions to retard the progression of an accident. Enhanced operator performance contributes significantly to overall system reliability and plant availability.

B. Recommendations

The system reliability analysis presented in this study was based on a point-estimate assessment for a one-hour interval upon a single demand to perform the system mission. The OAET is a qualitative treatment of the thermal-hydraulic responses to the transient initiator. The following are recommendations for future work related to this study:

1. Collect data of unscheduled outages of the nuclear plant due to transmission grid instabilities for a plant specific estimate of the probability of the LOSP frequency. The plant specific estimate contributes to better statistical accuracy in the analysis, and identifies plants for which the problem is most

serious. The plant specific estimate, being based on a single set of design parameters, has less uncertainty than a generic number.

2. Incorporate error factors in the reliability analysis to account for the uncertainty band surrounding every point estimate of a demand failure of a component. This provides the determination of system unavailability on a random variable basis. However, computer programs (e.g, SAMPLE-A, SPASM, etc.) using Monte Carlo random sampling techniques or other variance-estimating techniques, are required to obtain the distributions for the component failure estimates as input to the evaluation of the distribution of overall system unavailability.
3. Investigate the system unavailability for various time intervals, e.g., 4, 8 and 24 hours after event initiation, to assess time-dependent effects of the transient initiator.
4. Identify the core status and containment failure modes by means of containment damage and containment event trees. These event tree analyses identify the significant paths of radioactive release to the environment for the accident sequence. The identification of the significant release paths facilitates the estimation of fractional core inventory release to the environment during the course of the postulated accident.
5. Identify the key symptoms exhibited in the various plant states of the OAET so as to produce diagnostic algorithms. The diagnosis of key symptoms facilitates the development of improved

emergency procedures and the evaluation of plant instrumentation requirements.

IX. REFERENCES

1. Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400 (NUREG - 75/014). U.S. Nuclear Regulatory Commission, Washington, D.C., 1975.

2. D. C. Wood. Using Event Trees to Quantify the Effect of Post-TMI Modifications on PORV-Related LOCA Problems. Proceedings of ANS/ENS Topical Meeting on Probabilistic Risk Assessment 3(VIB), 1141-1150 (September, 1981).

3. N. J. McCormick. Reliability and Risk Analysis: Methods and Nuclear Power Applications. Academic Press, New York, 1981.

4. D. Okrent. Nuclear Reactor Safety. The University of Wisconsin Press, Madison, Wisconsin, 1981.

5. Analysis of Three Mile Island - Unit 2 Accident. Nuclear Safety Analysis Center Report. Electric Power Research Institute, Palo Alto, California. July, 1979.

6. F. L. Leverenz, G. McLagan and A. M. Azarm. Station Blackout: A Preliminary Assessment. SAI-102-81-AM, Report to NSAC. Electric Power Research Institute, Palo Alto, California. February, 1980.

7. W. E. Vesely. Failure Data and Risk Analysis. ANS Proceedings: Probabilistic Analysis of Nuclear Reactor Safety 2, (VI) 1.1-1.12 (May 1978).

8. B. B. Chu and D. P. Gaver. Availability Analysis for Some Standby Systems. ANS Proceedings: Probabilistic Analysis of Nuclear Reactor Safety 2, (VI) 8.1-8.14 (May, 1978).

9. A. Pages, M. Gondran and B. Magnon. Evaluation of the Reliability and the Availability of Large Repairable Systems by the Method of Critical Running States. ANS Proceedings: Probabilistic Analysis of Nuclear Reactor Safety 3, (VIII) 2.1-2.12 (May, 1978).

10. A. M. Azarm, G. McLagan, A. Husseiny and M. Metwally. Assessment of Diesel Generator Reliability in Light-Water Reactors. Am. Nuc. Soc. Transactions 35, 353-395 (November, 1980).

11. J. K. Vaurio. Availability Analysis of Standby Safety System. Proceedings of ANS/ENS Topical Meeting on Probabilistic Risk Assessment 2 (IVC), 707-716 (September, 1981).

12. T. Mankamo and U. Pulkkinen. Dependent Failures of Diesel Generators. Nuclear Safety 23(1), 32-40 (January, 1982).

13. D. G. Eisenhut. Reliability of D.C. Power Supplies in Nuclear Power Plant Application. ANS Proceedings: Probabilistic Analysis of Nuclear Reactor Safety 3, (XII) 8.1-8.10 (May, 1978).

14. E. W. Hagen. Technical Note: A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants. Nuclear Safety 23(1), 40-43 (January, 1982).

15. K. N. Fleming and P. H. Raabe. A Comparison of Three Methods for the Quantititative Analysis of Common Cause Failures. ANS Proceedings: Probabilistic Analysis of Nuclear Reactor Safety 3, (X) 3.1-3.12 (May, 1978).

16. R. G. Easterling. Probabilistic Analysis of Common Mode Failures. ANS Proceedings: Probabilistic Analysis of Nuclear Reactor Safety 3, (X) 7.1-7.12 (May, 1978).

17. J. A. Steverson and C. L. Atwood. Common Cause Failure Rate Estimates for Diesel Generators in Nuclear Power Plants. Proceedings of ANS/ENS Topical Meeting on Probabilistic Risk Assessment 2 (IVB), 659-665 (September, 1981).

18. F. E. Haskin, W. B. Murfin, J. B. Rivard and J. L. Darby. Analysis of a Hypothetical Core Meltdown Accident Initiated by Loss of Offsite Power for the Zion 1 Pressurized Water Reactor. Sandia Report (NUREG/CR-1988). Sandia National Laboratories, Albuquerque, New Mexico. December, 1981.

19. J. B. Fussell, J. S. Arendt, W. K. Crowley, D. P. Wagner, J. J. Rooney and D. J. Campbell. Improving System-Safety through Risk Assessment. Proceedings in 1979 Annual Reliability & Maintainability Symposium, 1979, 160-163 (January, 1979).

20. Y. G. Rosen and L. N. Nyh. Availability Study of Forsmark 3 Nuclear Power Plant. Proceedings in 1980 Annual Reliability & Maintainability Symposium, 1980, 70-75 (January, 1980).

21. H. Hoertner. Review on the Present Status of the German Risk Study-Plant Design Analysis. Proceedings of ANS/ENS Topical Meeting on Probabilistic Risk Assessment 3 (VIIB), 1334-1341 (September, 1981).

22. E. J. Henley and H. Kumamoto. Reliability Engineering and Risk Assessment. Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981.

23. M. L. Shooman. Probabilistic Reliability: An Engineering Approach. McGraw-Hill Book Company, New York, 1968.

24. Waterford 3 System Descriptions - AC Power Systems (SD-56). Louisiana Power and Light Company, Killona, Louisiana, 1982.

25. Waterford 3 System Descriptions - DC Power Distribution System (SD-58). Louisiana Power and Light Company, Killona, Louisiana, 1982.

26. Status Summary Reports for U.S. Licensed Operating Reactors (NUREG-0020). U.S. Nuclear Regulatory Commission, Washington, D.C., January, 1980 to November, 1982.

27. J. P. Poloski and W. H. Sullivan. Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants. EG&G Idaho Report (NUREG/CR-1362), Idaho Falls, Idaho, March, 1980.

A. Additional References

R. G. Brown, J. L. vonHerrmann and Y. F. Quilliam. Operator Action Event Trees for the Zion 1 Pressurized Water Reactor. EG&G Idaho Report (NUREG/CR-2888), Idaho National Engineering Laboratory, Idaho Falls, Idaho. September, 1982.

Emergency Operating Procedure: Loss of AC Power. Waterford 3 Plant Operating Manual 6(1), 1-12 (December, 1981).

PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants (NUREG/CR-2300). U.S. Nuclear Regulatory Commission, Washington, D.C., January, 1983.

Waterford 3 Final Safety Analysis Report - Chapter 15(2). Louisiana Power and Light Company, Killona, Louisiana, 1982.

S. M. Wong. Lecture Notes on AC Electrical Distribution for Waterford 3 General Systems Training Program. Louisiana Power and Light Company, Killona, Louisiana, 1983 (unpublished).

S. M. Wong. Lecture Notes on DC Power System for Waterford 3 General Systems Training Program. Louisiana Power and Light Company, Killona, Louisiaia, 1983 (unpublished).

X. ACKNOWLEDGMENT

Thanks be to God for His Grace and Blessings that this work reached its fruition.

The author expresses his sincere appreciation and gratitude to his major professors, Dr. Bernard I. Spinrad and Dr. Aly A. Mahmoud, for their useful discussions and guidance they provided throughout the preparation of this dissertation. In addition, the author expresses his special thanks to Dr. Randy L. Hagenson of the Los Alamos National Laboratory, New Mexico, for his constant encouragement and moral support under trying circumstances. Also, acknowledgment and a note of appreciation is due Dr. Zeinab A. Sabri of Louisiana Power and Light Company, who served initially as co-major professor.

Finally, the author dedicates this dissertation to the members of his immediate family in Malaysia. He also acknowledges the sincere and wonderful friendship of professional colleagues and operations personnel at the Waterford 3 Nuclear Plant during his sojourn as an onsite consultant in the Training Department of Louisiana Power and Light Company, Killona, Louisiana.

XI. APPENDIX. MONTHLY DATA OF FORCED OUTAGES FOR U.S. NUCLEAR POWER PLANTS IN COMMERCIAL OPERATION

Month	Forced Outages	Operating Units	Outage/Operating Unit
Jan. 1980	44	66	0.667
Feb. 1980	58	66	0.879
Mar. 1980	52	67	0.776
Apr. 1980	57	67	0.851
May 1980	61	67	0.910
Jun. 1980	65	67	0.970
Jul. 1980	64	67	0.955
Aug. 1980	71	66	0.930
Sep. 1980	60	66	0.909
Oct. 1980	52	66	0.788
Nov. 1980	62	66	0.939
Dec. 1980	61	67	0.910
Jan. 1981	49	67	0.731
Feb. 1981	55	67	0.821
Mar. 1981	58	67	0.866
Apr. 1981	59	67	0.881
May 1981	47	67	0.701
Jun. 1981	71	67	1.060
Jul. 1981	81	69	1.174
Aug. 1981	81	69	1.174
Sep. 1981	44	69	0.638

Month	Forced Outages	Operating Units	Outage/Operating Unit
Oct. 1981	69	70	0.986
Nov. 1981	56	70	0.800
Dec. 1981	67	70	0.957
Jan. 1982	83	71	1.169
Feb. 1982	56	71	0.789
Mar. 1982	52	71	0.732
Apr. 1982	72	71	1.014
May 1982	50	71	0.704
Jun. 1982	50	72	0.694
Jul. 1982	59	72	0.819
Aug. 1982	64	72	0.889
Sep. 1982	59	72	0.819
Oct. 1982	51	72	0.708
Nov. 1982	40	72	0.556

Average Forced Outage per Operating Unit in a Month = 0.862

Estimated Failure (Tripout) Rate of Main Generator = 1.159×10^{-3}/hr